

# SYSTEM SAFETY SCRAPBOOK

Ninth Edition



P. L. Clemens  
August 2002

**Sverdrup**

## — FOREWORD —

(This Foreword first appeared in the Sixth Edition.)

**BACKGROUND:** During the 1980s, Sverdrup Safety Office produced a series of “System Safety Scrapbook Sheets.” These Sheets were published on an as-needed basis, and each of them dealt with a single aspect of System Safety practice. As a series, their purpose was:

- to reinforce concepts presented in formal System Safety classroom training.
- to foster improved communication in matters of System Safety analysis.
- to sharpen basic “system savvy” and analytical skills.

As to their form, the Scrapbook Sheets were intentionally made quite casual, at times even whimsical. Emphasis was on meaning rather than style. The rules of proper syntax and the niceties of elegant convention were deliberately — some would say recklessly — set aside to further the more immediate purpose of conveying the message. And so, the readers of the Sheets encountered wholly unwarranted capitalizations, frequent lunges into italics, shotgun blasts of ellipses, and multiple underscorings and font shifts that would derange even the most calloused copy editor. But as to the *purpose*, it must be argued that it was, after all, exquisitely pure.

Publication of the Scrapbook Sheets was discontinued in late 1987 and resumed in 1995. Recipients of the Sheets often request reprints of Sheets that appeared early in the series. To satisfy that need and to preserve the complete set, the entire collection is reprinted in this form. The Scrapbook Sheets reproduced here represent the complete, original series together with recent additions. Other, newer sheets will appear in future editions of the Scrapbook.

**A CAVEAT:** The System Safety analyst is cautioned that the analysis process remains, at its best, an imperfect art. The “rules” of analysis that are declared or pretended will not ensure completeness. With perseverance, much of system risk may be recognized and controlled. But the recognition and the control will always be incomplete. Unrecognized elements of risk will always remain, in any system. And upon system operation, those undiscovered elements will have been accepted by default. The only alternative to this is unacceptable technological stagnation.

P. L. Clemens — May 1998

Sverdrup Technology, Inc.  
600 William Northern Blvd.  
Tullahoma, TN 37388  
(800) 251-3540  
[www.sverdrup.com/safety](http://www.sverdrup.com/safety)

**SYSTEM SAFETY SCRAPBOOK****— Table of Contents —**

<u>Topic</u>	<u>Sheet No.</u>
Single Point Failure Misconceptions.....	83-1
Critical Circuit FMEA Considerations.....	83-2
Resolving Disagreement between Redundant Readouts.....	83-3
Hierarchy of Countermeasure Effectiveness.....	83-4
Redundant Components vs. Redundant Systems.....	83-5
Fault Tree Analysis Review Hints.....	83-6
Countermeasure Selection Criteria.....	83-7
Failure Modes and Effects Analysis Review Hints.....	84-1
The “Risk Stream”.....	84-2
Labeling Hazards.....	84-3
The Importance of Probability Interval.....	84-4
The Isorisk Contour.....	84-5
PHA Shortcomings.....	84-6
A Hazards Checklist.....	86-1
A MORT Logic Flow.....	86-2
Operational Phasing.....	86-3
Common Causes: Diagnoses & Cures.....	86-4
Establishing the Fault-Tree Resolution Limit.....	86-5
Personnel & Procedures Present High Failure Probabilities.....	86-6
Fault Tree Diagnostic Aids.....	86-7
Fault Tree Nomenclature & Logic Rules.....	86-8
Four Risk Management Options.....	86-9
Avoiding Fault Tree Overgrowth.....	86-10
“Fault” & “Failure” Nomenclature.....	86-11
State-of-Component Method in Fault Tree Analysis.....	86-12
Inverting to Verify Fault Tree Logic — The “Flip-Top” Test.....	86-13
Making the Fault Tree “Top Box” Logic Exhaustive.....	86-14
Consider Cost & Feasibility with Competing Systems at Same Risk.....	86-15
Summary of Techniques: Application, Advantages, Shortcomings.....	87-1
Hints for Finding Hazards.....	87-2
Comparing Numerical Failure Probability with Real Life Events.....	87-3
Common Cause and the OR Gate.....	87-4
The Rare Event Approximation and OR Gates.....	87-5
On OR Gates, Success Domain, and the Exact Solution.....	87-6

...more 

— Table of Contents (continued...) —

<u>Topic</u>	<u>Sheet No.</u>
Getting Failure Probabilities from Reliability Data.....	95-1
The Bathtub Curve.....	95-2
MTBF Is Not Life Expectancy.....	95-3
“Scoping” to Bound Analyses.....	96-1
Preliminary Hazard Analysis Review Hints.....	96-2
The Thorough Analyst’s Penalty.....	96-3
Leapfrog Countermeasuring too often Deludes the Analyst.....	96-4
Requiring vs. Proving Low Failure Probabilities.....	97-1
Dealing with Probability Declaration Challenges.....	97-2
Converting MTBF to Failure Probability.....	97-3
“Equal” Risks may be Unequal.....	97-4
Bounding and Geometric Means to get Point Value Failure Probability.....	97-5
Reducing System Vulnerability.....	97-6
When to Revisit / Revise a Hazard Analysis.....	97-7
Preposterously Low Failure Probability?.....	97-8
Top-Down vs. Botom-Up Analyses.....	97-9
Hazard Inventory Techniques disguise Total System Risk.....	97-10
“Worst-Credible” Severity can be Misleading.....	97-11
Describing Hazards.....	98-1
Hazard Definition.....	98-2
“Types” and “Techniques” of Analysis.....	99-1
Risk Assessment for Human Targets.....	99-2
A Risk Assessment Matrix.....	00-1
“Calibrating” the Risk Assessment Matrix.....	00-2
Why worry over Fault Tree <b>TOP</b> Probability?.....	00-3
Quack Methods to Reduce Risk.....	00-4
Deciding Which Systems “Deserve” System Safety Analysis.....	00-5
Economic Aspects of System Safety.....	00-6
“Fault Tolerance” — A Sometimes Answer to Reducing Risk.....	00-7
Programmatic Risk — System Safety Methods will apply.....	01-1
Population affecting Severity and Probability.....	01-2
Exclusions from Preliminary Hazard Analyses.....	01-3
Assumptions regarding Client Care of analyzed systems.....	01-4
Precautions to take in reports to Clients.....	01-5
Disclaimers and Limitations.....	01-6

...more

## — Table of Contents (continued...) —

<u>Topic</u>	<u>Sheet No.</u>
Probability Estimating based on MTBF.....	01-7
Two functions of the Risk Assessment Matrix.....	01-8
Fault Tree Double-Talk to lower <b>TOP</b> Probability.....	01-9
Be wary of Lumping Targets.....	02-1
Reliability Engineering is not System Safety.....	02-2
If there've been no failures, what's failure probability?.....	02-3
How to prove system improvement.....	02-4
Is this system "safe?" .....	02-5
Fault Tree flimflamery.....	02-6
Fault Tree Modeling — <i>Functions</i> , not <i>Parts!</i> .....	02-7
Does Parts Swapout reduce Failure Probability?.....	02-8
Poisson Exponential Distribution vs. Sophisticated Analyses.....	02-9
A Long MTBF in a Short-Haul System.....	02-10
"Spreading" Risk may not reduce it.....	02-11
"Clustering" and Accident Prone-ness.....	02-12

— INDEX —

## — Single Points are EVIL —

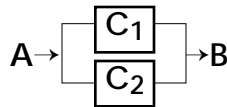
*...but High Failure Probability is Even WORSE!—*

**DEFINITION** — “A Single-Point Failure (SPF) is a failure of one independent element of a system which causes an immediate hazard to occur and/or causes the whole system to fail.” (*Professional Safety*, March 1981)

**PERCEPTION** — At first look, a potential SPF is a system evil! Redundancy is the remedy. That’s why, after all, we have two eyes, two ears, and two master brake cylinders. Sky divers wear two parachutes, squibs have multiple bridge wires, and airliners have co-pilots. A potential SPF makes a system vulnerable.

**REALITY** — Many systems contain potential SPFs but have remarkably high reliability. Behold, the basic automobile, a rolling cathedral of SPFs. There’s *one* ignition coil, fuel pump, fan belt, battery, distributor rotor, alternator, drive train, etc. The automobile is reliable because each of these potential SPF components has very low failure probability. Freedom from SPFs is a lot less important than *low overall failure probability*.

**EXAMPLE** — Consider a subsystem comprising a *single*, high-reliability component, **C**. Failure probability is correspondingly low — let’s say that  $P_F = 10^{-7}$  for a given mission. Because **C** is a potential SPF, we fear its effect on system vulnerability.



We replace that single **C** with two, parallel-redundant components. Now, the SPF is gone. But did cost considerations cause us to select the new **C<sub>1</sub>** and **C<sub>2</sub>** components with higher individual failure probability for the same mission? ...say,  $P_C = 10^{-3}$ ? In *this* case, the new redundant  $P_F = 10^{-6}$  is worse than for the SPF component we replaced! AND, *have* we truly saved money? We now have two *el cheepo* components to *maintain* and to *replace*. (Probably they must be replaced more frequently.) If one fails, unless there’s an inspection process or an alarm to warn us that there’s only one more component to go, the remaining  $P_F$  is now very high! And we’re *back* to an SPF without knowing it! AND, are both components vulnerable to the same *common cause* of failure? (See Scrapbook Sheet 86-4.) E.g., can the same moisture that fails **C<sub>1</sub>** also fail **C<sub>2</sub>**? Our “improved” SPF-free system now begins to look a lot worse!

### BOTTOM LINE

Single-point failures deserve the system analyst’s attention! But in the end, it’s overall system failure probability that counts, whether this is controlled by redundancy or by other means. A *Single-Point Failure*, like the music of Wagner, may not be as bad as it sounds!

## — Example Failure Modes and Effects Considerations for Critical Circuits —

- **SWITCHES:** 1. Fail to Open 2. Fail to Close 3. Close Partially (High Resistance)
- **RELAYS:** 1. Slow to Open 4. Contacts “Freeze” Closed (Mechanically or by Overcurrent)  
2. Slow to Close 5. Contacts Fail to “Make” (or Make on High Resistance)  
3. Coil Burnout 6. Contacts “Bounce” (Erratic/Repeated “Makes”)
- **CONNECTORS:** 1. Pin-to-Pin “Short” (or Low Resistance)  
2. Pin-thru “Open” (or High Resistance)
- **FUSES:** 1. Open on Undercurrent 2. Fail to Open on Overcurrent (or Slow to Open)  
3. Open Partially (Provide Leakage Path)
- **SIGNALS/  
PULSES:**

1. Too Early	6. Wrong Frequency
2. Too Late	7. Wrong Phase
3. Too Long	8. Noisy
4. Too Brief	9. Source Impedance too High
5. Wrong Polarity	10. Source Impedance too Low
- **DIODES:** 1. Fail “Open” 2. Fail “Short” 3. Loss of Front-to-Back Ratio
- **HUMAN OPERATOR  
FUNCTION:**

1. Too Early	5. Out of Sequence
2. Too Late	6. Omitted
3. Too Long	7. Two at Once
4. Too Brief	8. Right Act/Wrong Target

### *BOTTOM LINE*

Components can fail in Many Ways! Identifying each way and exploring its consequences to the system is what Failure Modes and Effects Analysis is all about!  
But beware of guides like this one ...*NO CHECKLIST IS EVER COMPLETE!*

## — Redundant Readouts Disagree?

*...Pessimism Wins!—*

- **BACKGROUND** — Redundant readout is a feature found in many control systems. The redundancy may be provided in a variety of ways. Two distinctly separate channels may be provided, for example, each with its own sensor, signal processing equipment, and output display. The sensors may operate on physically different principles, and the channels may derive power from separate sources. (These are desirable attributes for redundant systems.) At the opposite extreme is the case of redundant readout for which only a single element may be duplicated — e.g., the output display, which may be reproduced for personnel in widely separated control rooms.
- **POTENTIAL PROBLEM** — When redundant readouts differ and one shows an out-of-bounds reading, human operator reaction is often to discredit the out-of-bounds reading in favor of the apparently “normal” one. The readout difference sometimes leads to a period of protracted contemplation or discussion during which attempts are made to resolve the difference. System performance, however, may actually *be* out of bounds, and time may be lost which might otherwise be devoted to regaining system control or to initiating safe shutdown procedures. This phenomenon is a trait of many major disasters.
- **CURE** — Operator reactions to out-of-bounds readings by *any* monitoring instrument should be based on the presumption that the instrument is performing properly, unless there is immediate persuasive evidence that it is *not* performing properly. This philosophy should prevail *whether or not* another measurement channel or readout device appears to provide assurance that system performance is acceptable.

### *BOTTOM LINE* —

Redundant Readout, in and of itself, is NOT a system “evil,” but an often-desirable feature. It affords freedom from potential single-point oversight of system malfunction ...but *only* if it is BELIEVED! *It is better to answer a dozen false alarms than to allow one house to burn to the ground!*



## — Effectiveness of Countermeasures of Diverse Kinds —

*...some mitigation methods are mightier than others!*

When seeking to reduce RISK by lowering PROBABILITY  
or SEVERITY or BOTH, rank prospective COUNTERMEASURES thusly\*:

- ↑ INCREASING EFFECTIVENESS
- **DESIGN** — Adopt a design that excludes the hazard. *If the hazard is FLOODED BASEMENT, place the basement floor above the water table.*
  - **ENGINEERED SAFETY FEATURES** — Use redundant backups, automatic preventers/correctors, interlocks. (Active Devices) *Install a sump, with pumps operated by a float switch.*
  - **SAFETY DEVICES** — Use guards, shields, suppressors. (Passive Devices) *Waterproof the basement walls and floor, and use check valves in floor drains.*
  - **WARNING SYSTEMS** — Use audible/visual alarms and signals to trigger avoidance reactions or corrective responses. *Use horns, bells, lights operated by a float switch or moisture detector.*
  - **PROCEDURES AND TRAINING** — Develop/implement work methods which control risk. Provide training in them. *Formulate inspection procedures and emergency bailing plan; train personnel in their use.*

\*Adapted from MIL-STD-882D and MIL-STD 1574

### NOTE:

- Exceptions to this effectiveness hierarchy do arise in practice.
- Some hazards may deserve several countermeasures, perhaps at several levels; e.g., Warning Systems are seldom effective without Procedures and Training.
- Some countermeasures are difficult to classify according to this hierarchy — e.g., frequent parts replacement to stretch **MTBF**.
- Avoid adopting countermeasures that introduce new hazards or that impair system performance.
- For competing countermeasures at the same effectiveness level, let *feasibility* (including schedule) and *cost* decide the winner(s).

### BOTTOM LINE

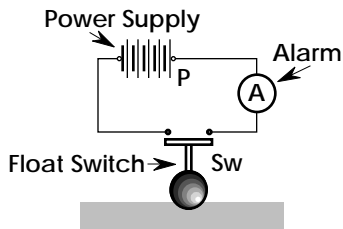
Countermeasures against risk are of various kinds. Their effectiveness varies from kind to kind. *It is better to slay a dragon than to teach people ways to live peacefully with him! ...a little riddance is better than a lot of accommodation!*

## — Several Routes to Redundancy...

### SELECT with CARE! —

Redundancy is often used to reduce system vulnerability. There are various ways to apply redundancy. They are not equally effective. For example, consider the alternatives of ① duplicating the entire system and ② duplicating the components within the system:

#### BASIC SYSTEM —



A flood alarm system uses a float switch, as shown. What is the probability ( $P_T$ ) that, if flooding occurs, it will *not* be annunciated? ...assume each component (P, A, Sw) fails once in each  $10^3$  demands:

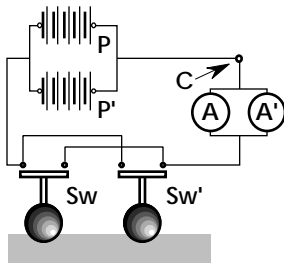
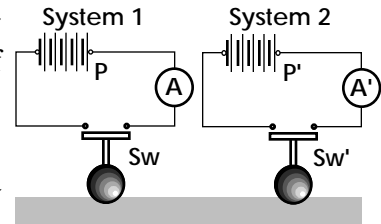
$$P_T = P_P + P_A + P_{Sw} = 3 \times 10^{-3}$$

The system will fail three times in each 1000 demands, on long-term average. Too many? Go redundant!

① **DUPLICATE SYSTEMS** — Use two, identical, wholly independent redundant systems. Now the probability of annunciation failure becomes substantially lower:

$$P_T = P_1 \times P_2 = 9 \times 10^{-6}$$

Failure probability has been reduced by  $0.3 \times 10^3$  ...a gratifying outcome!



② **DUPLICATE COMPONENTS** — BUT, suppose we duplicate components *within* the original Basic System? For this case:

$$P_T = P_P^2 + P_A^2 + P_{Sw}^2 = 3 \times 10^{-6}$$

NOW, failure probability is  $10^3$  lower than for the Basic System and one third of that for the Duplicate System case — less vulnerability, *using the same components!*

**WHAT HAVE WE OVERLOOKED?** Think about *Common Causes!* (See Scrapbook Sheet 86-4.) Suppose corrosion opens the circuit at point C? Or rising water disables the power supplies before closing the float switches? Or mud daubers bugger both side-by-side float switches? These Common Cause considerations *can* favor using two, wholly independent, location-separated, redundant Basic Systems! (Still better for immunity to Common Cause afflictions: use redundant components having differing operating principles.) Think also about *Component Fratricide*. If either power supply fails in short circuit mode, it kills its brother power supply!

#### BOTTOM LINE —

Whole-system redundancy is not always better than the redundancy given by duplicating the components within the system. *For some operations, you may be better off with extra pots and pans than with a complete spare kitchen!*

KNOW THY SYSTEM!

## — Fault Tree Review Hints —

- Is TOP box “scoping” appropriate? (Consider: Time/Duration; Activity/Function/Application; Loss Penalty/Severity; Place/Space; Life Cycle; Mission Phase; etc.)
- Are all box statements (i.e., “headlines”) unambiguous *fault* events or conditions?
- Does each box statement represent *one discrete* event or condition?
- Are all elements immediately below a given gate *independent* of one another?
- Is logic preserved? — i.e., are all the elements immediately below each gate *BOTH...*
  - ① *Necessary* (Do they truly contribute to opening the gate?)  
...AND...
  - ② *Sufficient* (Are there missing elements?)  
...to open the gate above?
- Are there “illegal” gate-to-gate shortcut connections? (Don’t let a gate feed a gate!)
- Are appropriate *Common Causes* represented? (Scrapbook Sheets 86-4 and 87-4)
- Is the *Probability Interval* specified? (Duration or number of operations — Scrapbook Sheets 84-4 and 99-2.)
- Do *Probability Values* have a common basis? (Don’t “mix” units — don’t dilute actuarial data with subjective estimates without justifying.)
- Have *Cut Sets* been determined? (Would they aid system analysis?)
- Have *Path Sets* been determined? (Would they aid system analysis?)
- Has a *Sensitivity Analysis* been performed? (Would it disclose system vulnerability?)
- Is Operational Phasing accounted for? (Scrapbook Sheet 86-3)
- Are *Human Operator* functions/interactions accounted for?
- Are there *Man Paths* to the TOP? (They signal high vulnerability!)
- Are *External Causes* represented? (Think meteorology/seismology/etc.)
- Is the Tree an *accurate conceptual model* of the System?

### BOTTOM LINE

The fault tree uses tools of logic to model the system and to guide the analysis of paths to system failure. The model must be realistic and the tools must be properly used. *If you lie to the Tree, the Tree will lie to you!*

## — Selection Criteria for Risk Control Countermeasures —

*When considering COUNTERMEASURES  
against RISK,  
use these three equally important  
SELECTION CRITERIA...*

- **EFFECTIVENESS** — Does the Candidate Countermeasure *adequately control* Risk? ...by reducing Probability and/or Severity ...and without compromising System Performance ...and without introducing New Hazards that also have unpleasant Risk?
- **FEASIBILITY** — *Can* the Candidate Countermeasure be *applied* ...and on an acceptable *time schedule*?
- **COST** — Can the *cost* of the Candidate Countermeasure be supported, as opposed to the probable cost of accepting the Risk? Consider *all aspects of Cost* — Initial Outlay, Installation, Operation, Maintenance, Decommissioning, etc.

---

**DON'T "OVERKILL" A Hazard's RISK!** — To do so robs resources that might be devoted to controlling other more deserving cases!

### *BOTTOM LINE*

If you pick a Countermeasure that won't do the job, or that's impossible to use or to apply soon enough, or that's unaffordable, you'll end up in partnership with the very risk you'd sought to subdue. *Consider alternative Countermeasures; pick one(s) that'll handle the Hazard, that you can afford, and that you can apply!*

## — Failure Modes & Effects Analysis Review Hints —

*...so you've done an FMEA — has it done these things?*

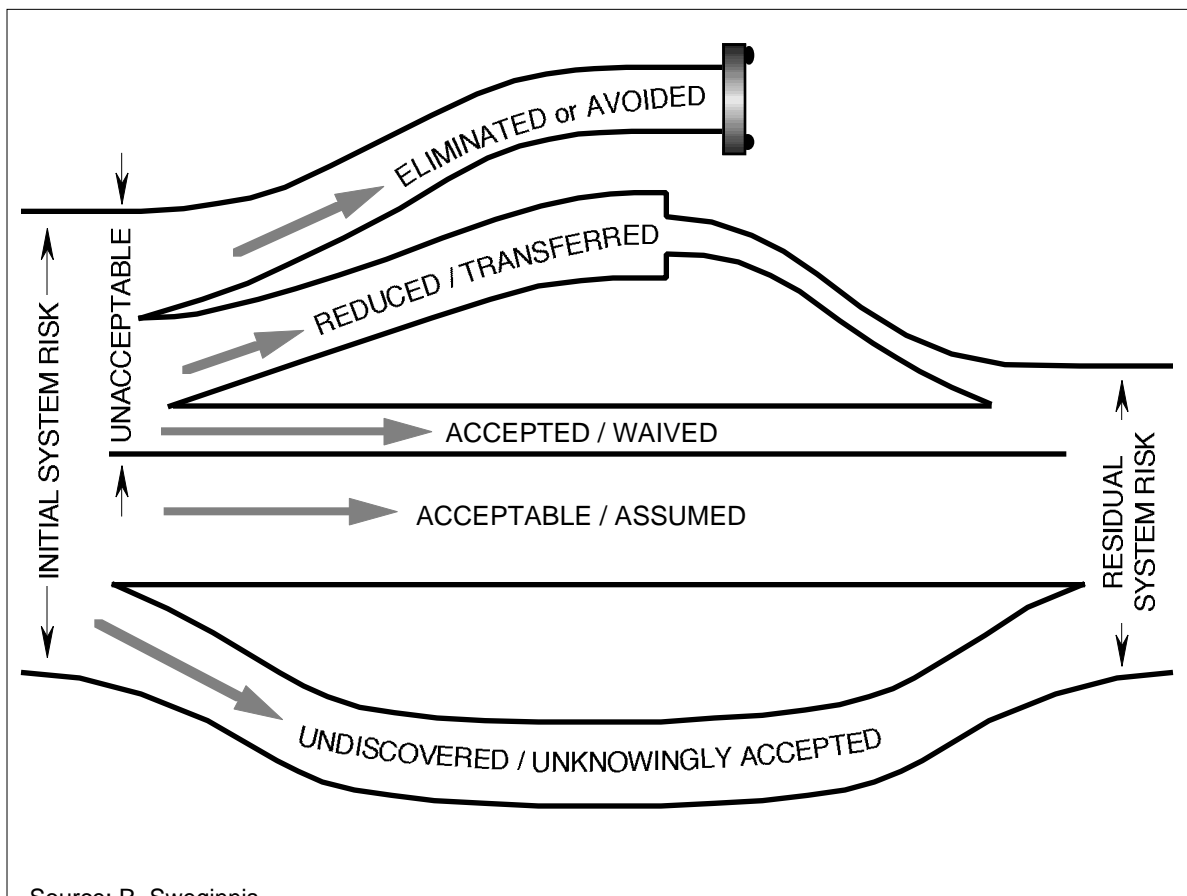
- Has the System to be analyzed been defined/bounded? (See Scrapbook Sheet 96-1.)
- Has a Probability Interval been declared? (See Scrapbook Sheet 84-4.)
- Has the System been divided into well-differentiated Subsystems, Assemblies, Subassemblies, etc.?
- Has a System Block Diagram been constructed to guide the analysis?
- Has a components list for each subsystem been prepared?
- Is the specific function of each component known?
- Has a comprehensive coding/identification system been established?
- Have all reasonable *failure modes/causes/effects* been considered for each item listed?
- Has it been assumed (*erroneously!*) that items will fail only in modes of design intent?
- Have interface items and their failure modes been dealt with?
- Have utility and support features been treated?
- Have latent failure modes been considered? (Item in initial fault state from prior use.)
- Are Operational Phases recognized/differentiated? (See Scrapbook Sheet 86-3.)
- Is the “Action Required” for control of unacceptable failure modes adequate?
- Are *Risk Assessments* correct? (if used)
- Have worksheet “*headline*” *information/signature blocks* been completed/dated?
- Have proper *identification numbers* from the coding system been used?
- Are System *item functions* properly identified?
- Are means of failure detection/annunciation elucidated?
- Is the Worksheet itself sufficiently detailed and complete to cover the system being analyzed?
- Is the analysis summarized so as to include conclusions, criticality ranking, and necessary recommendations?

### *BOTTOM LINE*

Like other System Safety analytical methods, FMEA will only work as hard for you as you work for it! Only thoroughness yields thoroughness! And, as with other hazard analysis methods...if you don't know about it, you won't look for it, and if you don't look for it, you won't find it...IT'LL find YOU!

## — The RISK STREAM ...a Useful Concept —

**Elements of RISK** that characterize the hazards found in any system/activity/mission can be represented by a RISK STREAM. Some of the total risk will be acceptable. Some will not. Of that part which is not acceptable, some can usually be eliminated or avoided. Some can also be reduced, making it acceptable. Often, some of the risk originally viewed as unacceptable must, in fact, be tolerated if the system is to be operated. And in any system, no matter how well engineered and no matter how thoroughly analyzed, there will always remain residual risk, some of which will have gone undiscovered.



### *BOTTOM LINE*

System Risk is a stream, of several branches. Some are peaceful and still. Others are turbulent and treacherous. Some can be dammed or narrowed. But a few rapids will always remain, some of them hidden. You'll be taking trips up all of them. *Be sure to bring your paddle!*

# — Assessing RISK?

## ...when is a HAZARD a HAZARD? —

*Don't let the "naming" become confused with the concept!*

- **SYSTEM SAFETY ANALYSIS** often starts with a straightforward listing of HAZARDS. A hazard is simply a threat of harm. RISK ASSESSMENT follows. It consists of evaluating the SEVERITY of the harm and the PROBABILITY that the harm will result. Often we name a hazard according to the the *severity* component of its risk. In doing this we are describing a particular *consequence* of the hazard rather than the hazard itself. This can be misleading! It distracts us from considering *other* possible consequences and *their* probabilities.
- **EXAMPLES:** In analyzing the transportation system you use commuting to work, you identify the hazard "Fatal Highway Crash." Because you can ponder probability and can spot prospective causes (e.g., excess speed, worn tires, driver inattention, road surface irregularities, etc.) that Fatal Highway Crash *seems* like a hazard, It's *not!* Its name conveys severity (a fatality), and it's a *consequence* of one or more of the real hazards at work — perhaps involving that excess speed and those worn tires.

Here are some other cases where people practicing system safety have identified a *consequence* when they thought they were listing a real hazard. Notice how mis-naming the hazard discourages consideration of other consequences. Notice, also, that each Real Hazard could *have* other consequences!

<b>PSEUDO HAZARD</b> <u>(A Consequence)</u>	<b>THE REAL HAZARD</b> (Find <i>Other</i> Consequences!)
• Fall Injury.....	Unprotected Excavation
• Electrocution.....	Exposed Energized Conductor
• Hearing Damage.....	Explosive Mixture

- **USEFUL PRACTICE:** Make the description of each hazard tell a miniature story — a little scenario that addresses the Source, the Mechanism, and the Outcome\* (i.e., Consequences) that characterize the harm that is threatened by the hazard. Example: Worn tires leading to blowout at high speed resulting in loss-of-control crash and driver fatality.

\*See Scrapbook Sheet 98-1.

### *BOTTOM LINE*

Have you labeled a *hazard*, or have you labeled the *disaster* it produces? When you name a hazard, be sure it *is* the hazard and not a consequence! Then look for *all* of its real, potential consequences. However, it's better to *find* the hazards, to *assess* their risks, and to *impose countermeasures* for intolerable ones than it is to spend energy developing elegant names for them!

## — Assessing RISK?

...EXPOSURE INTERVAL\* is *IMPORTANT!*—

*It matters how many times you plan to roll those dice!*

### LEARNED LINGO

**SYSTEM SAFETY ANALYSIS** requires recognizing System Hazards, followed by assessing Risk for those hazards. The hazards themselves are conditions or operations that have potential to cause *harm* i.e., they are simply *threats* to things of value. (See Scrapbook Sheet 98-2.)

For each hazard, RISK is a *doublet!* Its components are PROBABILITY and SEVERITY. Probability is the *likelihood* that the hazard will result in harm, and SEVERITY is the *magnitude* of that harm, conventionally evaluated at its worst-credible level. Probability and severity depend upon different physical aspects of the hazard. **IMPORTANT:** That probability component of risk has meaning *only* if it is associated with operating duration or a specific number of operations that represent system exposure to the hazard!

### HOMIEY EXAMPLE

**TO DEMONSTRATE,** consider your car and the hazard “worn tires in highway use.” *Severity* of a blowout mishap depends upon such factors as vehicle speed, number of passengers, degree of passenger protection, presence of roadside obstacles, and driver competence. *Probability* may be a function of some of these same factors (e.g., vehicle speed), but it also involves other factors such as degree of tire wear, road surface condition, tire inflation level, and ambient temperature. **IMPORTANT:** Probability is *also* a function of the number of miles to be driven, i.e., the exposure interval, mission duration, or probability period. (It is called by many names.) This explains why your auto insurance premium is greater for a full year than for a single month. Increasing the exposure interval increases the probability component of risk!

### BOTTOM LINE

Don't talk about RISK without talking about PROBABILITY and SEVERITY. And don't talk about PROBABILITY without talking about EXPOSURE INTERVAL! *The probability of flipping a coin and getting a tail is 50%...but only if you flip the coin just one time! For a two-flip mission, it's 75% ...and for a three-flip mission, it's 87.5% ...and ...*

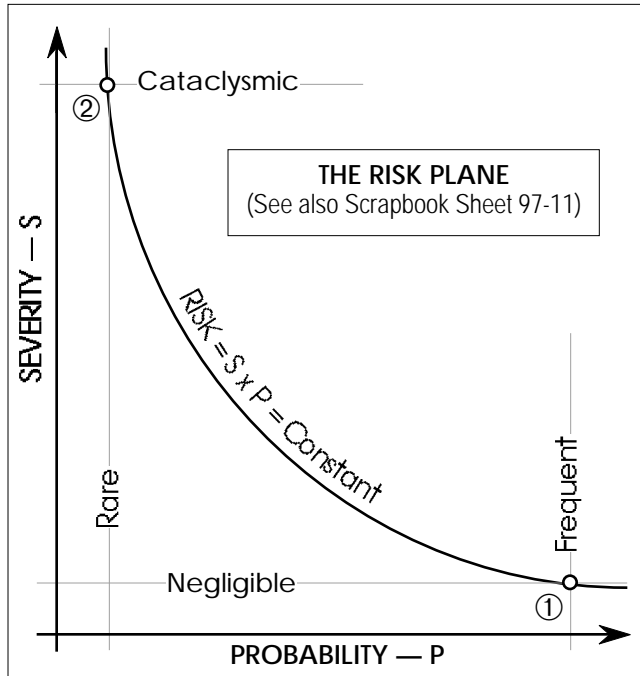


— Once Risk is *Assessed*,  
 ...it *STAYS* That Way! — (*mostly*) —

The Iso-Risk Contour is a Help to Understanding!

- **MANY HAZARDS** display a useful natural property. (A hazard is simply a threat of *harm*; see Scrapbook Sheet 98-2) For many hazards, the *Risks* for multiple available outcomes are more-or-less equal! Risk is simply the product of *Severity* and *Probability*.

All risks that lie along a constant  $R = S \times P$  contour are of equal magnitude. Risk for many hazards is described by such a contour. Even though the individual outcomes that can be produced by the hazard may have varying degrees of Severity, the *products* of Severity and Probability for the various outcomes of the same hazard are relatively constant.



- **SIMPLE EXAMPLE** — Consider the hazard “unprotected skin exposure to a sharp-edged instrument while shaving.” Negligible nicks occur frequently (High Probability/Low Severity — Point ①). In a very few cases, infection occurs, leads to blood poisoning, treatment fails, and death follows (Point ②). Along the contour from ① to ② are worsening levels of outcome at diminishing probability: brief minor infection, hospitalization, lasting disfigurement, etc., each having about the same level of  $R = S \times P$ .

- **WATCH OUT!** — Not all hazards behave this way! Consider the hazard “unprotected hand exposure to 68-KV transmission line.” Risk for such a hazard can be represented by a single point in the Risk Plane rather than by a continuous contour. Severity is deadly. Probability is determined by the characteristics of the setting.

*BOTTOM LINE*

For many hazards, once you’ve assessed *risk* for *one* consequence, it holds for *all others*. But ...there are *exceptions*. Don’t get caught on a High-Voltage **EXCEPTION!**

— ***PRELIMINARY HAZARD ANALYSIS...***  
**an Important Tool**  
**with a Few *Shortcomings!***—

- **PRELIMINARY HAZARD ANALYSIS (PHA)** is an important System Safety Tool! It produces a hazard-by-hazard inventory of system hazards and an assessment of the risk of each of them. A PHA is also a *screening* or *prioritizing* operation. It helps separate hazards that pose obviously low, acceptable risk from the intolerable ones for which countermeasures must be developed. *And*, it can help to identify the need for analysis by another System Safety technique.
- **FOR A COMPLEX SYSTEM** made up of many interrelated elements, a PHA often just won't hack it! A PHA does not readily recognize calamities that can be brought about by co-existing faults/failures at scattered points in a system, for example. A more complex analysis by another method may be needed for such a case.
- **THOROUGHNESS IS IN DOUBT** for the PHA — for *any* PHA — and this is because the methods of *finding* the hazards all rely on applying *subjective* aids such as checklists, walkthroughs, and application of intuitive skills. Thus, no PHA can ever be relied upon to list *all* system hazards.
- **NATURE SUMS RISKS** for system hazards, whereas the PHA views them individually. Consider a PHA that has identified a large population of hazards. Risk may have been assessed as being acceptable for each of them. This leads to the supposition that overall system risk is also acceptable. However, *true total system risk* is more nearly the *sum* of all those independent partial hazard-by-hazard risks! (See Scrapbook Sheet 97-10.) Suppose the large number of hazards is  $n$ , and that mishap probability for each of them is very low (say  $1/n$ ). The probability ( $P_T$ ) that one of the hazards will produce a system mishap becomes very close to unity, even though each individual hazard may seem to pose minor risk:

$$P_T = \frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} + \dots + \frac{1}{n} \approx 1.0$$

A NASTY EVENT is **GUARANTEED!**

***BOTTOM LINE*** —

A PHA is a GREAT starting spot for System Safety. It'll produce an itemized list of hazards for straightforward systems. It'll often point the way to needs for more advanced analyses. BUT ...*distrust* it for large or complex systems! It'll lie about overall system risk! *Even a great looking grocery list can leave you with a lousy stew on your hands!*

# — An Incomplete\* CHECKLIST of ASSORTED HAZARDS —

*...for use in Preliminary Hazard Analyses and Design Reviews*

**Here's a partial\* list of types of Hazards to consider in conducting the important search for hazards in your very own System!**

## — System Safety Hazards Checklist —

### • **Electrical**

- Shock
- Burns
- Overheating
- Ignition of Combustibles
- Inadvertent Activation
- Power Outage
- Distribution Backfeed
- Unsafe Failure to Operate
- Explosion/Electrical (Electrostatic)
- Explosion/Electrical (Arc)

### • **Mechanical**

- Sharp Edges/Points
- Rotating Equipment
- Reciprocating Equipment
- Pinch Points
- Lifting Weights
- Stability/Toppling Potential
- Ejected Parts/Fragments
- Crushing Surfaces

### • **Pneumatic/Hydraulic Pressure**

- Overpressurization
- Pipe/Vessel/Duct Rupture
- Implosion
- Mislocated Relief Device
- Dynamic Pressure Loading
- Relief Pressure Improperly Set
- Backflow
- Crossflow
- Hydraulic Ram
- Inadvertent Release
- Miscalibrated Relief Device
- Blown Objects
- Pipe/Hose Whip
- Blast

...more 

#### *BOTTOM LINE*

**\*NO HAZARD CHECKLIST SHOULD BE CONSIDERED COMPLETE!** This one is meant *only* as a Basic Starter Kit. Enlarge it and tailor it as experience is gained in its use. And *NEVER* rely on a checklist alone as a means of identifying System Hazards!

• **Acceleration/Deceleration/Gravity**

- Inadvertent Motion
- Loose Object Translation
- Impacts
- Falling Objects
- Fragments/Missiles
- Sloshing Liquids
- Slip/Trip
- Falls

• **Temperature Extremes**

- Heat Source/Sink
- Hot/Cold Surface Burns
- Confined Gas/Liquid
- Pressure Elevation
- Elevated Flammability
- Altered Structural Properties (e. g., Embrittlement)
- Elevated Reactivity
- Freezing
- Reduced Reliability
- Humidity/Moisture
- Elevated Volatility

• **Fire/Flammability**

Presence of:

- Fuel
- Oxidizer
- Ignition Source
- Propellant

• **Radiation**

Ionizing

- Alpha
- Beta
- Neutron
- Gamma
- X Ray

Non-Ionizing

- Laser
- Infrared
- Microwave
- Ultraviolet

• **Explosives**

Initiators:

- Heat
- Friction
- Impact/Shock
- Vibration
- Electrostatic Discharge
- Chemical Contamination

Sensitizers:

- Heat/Cold
- Vibration
- Impact/Shock
- Low Humidity
- Chemical Contamination

...more 

• **Explosives (continued)**

- Lightning
- Welding (Stray Current/Sparks)
- Radio Frequency Energy
- Induced Voltage (Capacitive Coupling)

Effects:

- Mass Fire
- Blast Overpressure
- Thrown Fragments
- Seismic Ground Wave
- Meteorological Reinforcement

Conditions:

- Explosive Propellant Present
- Explosive Gas Present
- Explosive Liquid Present
- Explosive Vapor Present
- Explosive Dust Present

• **Leaks/Spills**

Materials:

- Liquids/Cryogenics
- Gases/Vapors
- Dusts
- Radiation Sources

Conditions:

- Flammable
- Toxic
- Irritating
- Corrosive

- Slippery
- Odorous
- Reactive
- Asphyxiating
- Flooding
- Run Off
- Pathogenic
- Vapor Propagation

• **Chemical/Water Contamination**

- System Cross-Connection
- Leaks/Spills
- Vessel/Pipe/Conduit Rupture
- Backflow/Siphon Effect

• **Physiological (Also see Ergonomic)**

- Temperature Extremes
- Baropressure Extremes
- Fatigue
- Lifted Weights
- Noise
- Carcinogens
- Vibration (Raynaud's Syndrome)
- Nuisance Dusts/Odors
- Asphyxiants
- Allergens
- Pathogens
- Radiation (Also see **Radiation**)
- Cryogenics
- Mutagens
- Teratogens
- Toxins
- Irritants

• **Human Factors (Also see Ergonomic)**

- Operator Error
- Inadvertent Operation
- Failure to Operate
- Operation Early/Late
- Operation Out of Sequence
- Right Operation/Wrong Control
- Operate Too Long
- Operate Too Briefly

• **Ergonomic (Also see Human Factors)**

- Fatigue
- Inaccessibility
- Inadequate Control/Readout Differentiation
- Inappropriate Control/Readout Location
- Faulty/Inadequate Control/Readout Labeling
- Inadequate/Improper Illumination
- Glare
- Nonexisting/Inadequate "Kill" Switches
- Faulty Workstation Design

• **Control Systems**

- Power Outage
- Interference (EMI/ESI)
- Moisture
- Sneak Circuit
- Sneak Software
- Lightning Strike
- Grounding Failure
- Inadvertent Activation

• **Unannounced Utility Outages**

- Electricity
- Steam
- Heating/Cooling
- Ventilation
- Air Conditioning
- Compressed Air/Gas
- Lubrication
- Drains/Sumps
- Fuel
- Exhaust

• **Common Causes**

- Utility Outages
- Moisture/Humidity
- Temperature Extremes
- Seismic Disturbance/Impact
- Vibration
- Flooding
- Dust/Dirt
- Faulty Calibration
- Fire
- Single-Operator Coupling
- Location
- Radiation
- Wear-Out
- Maintenance Error
- Vermin/Varmints/Mud Daubers

• **Contingencies**

Emergency responses by System/Operators to "unusual" events:

- "Hard" Shutdowns/Failures
- Freezing
- Fire
- Windstorm
- Hailstorm
- Utility Outages
- Flooding
- Earthquake
- Snow/Ice Load

• **Mission Phasing**

- Transport
- Delivery
- Installation
- Calibration
- Checkout
- Shake Down
- Activation
- Standard Start
- Emergency Start
- Normal Operation
- Load Change
- Coupling/Uncoupling
- Stressed Operation
- Standard Shutdown
- Emergency Shutdown
- Trouble Shooting
- Maintenance
- . . . all others . . . (?)

————— end\* —————

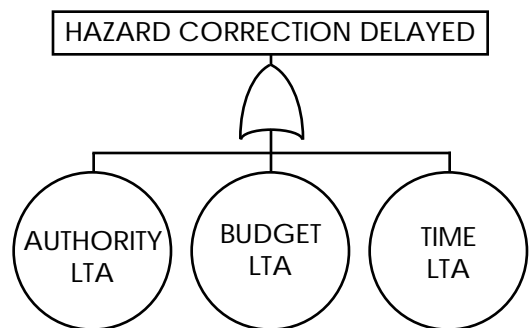
\*...but *NO* Hazard Checklist *ever* really ends!

## — Using *MORT*?

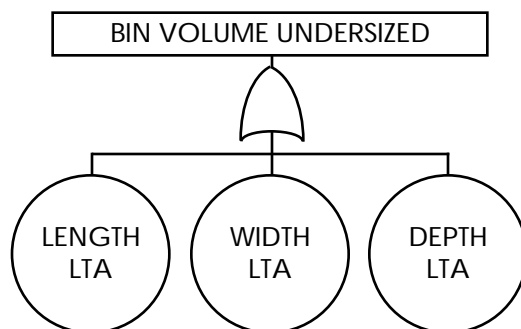
### ...watch out for that *LOGIC FLAW!*—

#### Words of Caution for the MORT-icians amongst us

- **BACKGROUND** — MORT (Management Oversight & Risk Tree analysis) is often used as a non-quantitative System Safety tool. The all-purpose, pre-cooked logic tree which serves as the basis for MORT is *exhaustively thorough!* The tree is of great value in mishap investigation and is also useful as a subjective “comparator” against which to gage safety program effectiveness.
- **LOGIC FLAW** — The MORT tree relies upon an analytical gimmick that, though useful, harbors a logic shortcoming. Most of the tree “initiators” (i.e., the basic events/conditions) are modified by the *indefinite descriptor* “Less Than Adequate” (LTA). These LTA initiators are arrayed beneath OR gates. This logic overlooks the reality that a super-sufficiency in one system attribute may offset deficiencies (LTAs) in the complementary attributes.
- **EXAMPLE** — A typical MORT element deals with uncorrected hazards. Insufficient AUTHORITY OR BUDGET OR TIME are shown to result in delays in hazard correction. This ignores the potential for a *more-than-adequate* budget to overwhelm possible shortfalls in TIME (i.e., correction schedule).



Suppose that Less-Than-Adequate Bin Volume is the undesired event/condition. If any two of the contributing bin attributes



(Length/Width/Depth) are greater than zero, then sufficient magnitude of the third attribute will produce any desired level of bin volume. Thus, the MORT descriptor LTA, used in conjunction with the OR gate, becomes meaningless. (It’s also uncertain whether the logic gate should be OR or AND.)

- **RESULT** — In many analyses, this Logic Flaw will *over-estimate* System vulnerability. That is, as a diagnostic device, MORT is sometimes *unrealistically pessimistic*. However, if an “ultraconservative” analysis is wanted, this property of the MORT tree becomes an *advantage!*

#### *BOTTOM LINE*

MORT’s useful. But *be wary* of those indefinite “Less-Than-Adequate” OR gates!

Don’t get MORT-ified into under-rating your System!



## — Doing a *HAZARD ANALYSIS?* think *OPERATIONAL PHASE*—

Checking the System for Symptoms when it's *Healthy*  
won't disclose it's *Next Disease!*

- **THE PROBLEM** — For the usual system, hazards and their risks vary from operational phase to operational phase. (An operational phase is a functionally discrete portion of system life cycle.) *Most* system failures occur *not* during the phase when the system is “up” and running normally, doing its intended thing. Failures more often occur during a start-up or a shut down or a load change or a maintenance “transient.” BUT ...*most* System Safety *analyses* treat *only* the full-up system, running steady-state, as intended, at nameplate rating. *SEE THE FLAW?*
- **THE CURE** — To be thorough, System Safety analyses must consider the hazards and risks peculiar to each of the operating phases that can be occupied by the system. Some hazards may be unique to certain phases. And for some hazards that are present during several phases, the risk may vary from phase to phase, requiring a separate consideration for each of the phases. (See below.)
- **SOME OPERATIONAL PHASE EXAMPLES** —
  - Transport
  - Delivery
  - Installation
  - Calibration
  - Checkout
  - Shake Down
  - Activation
  - Standard Start
  - Emergency Start
  - Normal Operation
  - Load Change
  - Coupling/Uncoupling
  - Stressed Operation
  - Standard Shutdown/Stop
  - Emergency Shutdown/Stop
  - Trouble Shooting
  - Maintenance
  - ...all others...?

### *BOTTOM LINE*

Things rarely go wrong when everything's running as it should. *The law of Status Quo*: If nothing *changes*, everything will be the *same*. *1<sup>st</sup> Corollary*: If something *changes*, things'll be *different*. *Unexpected failure* is an *annoying difference* to have to put up with!

## — The COMMON CAUSE FAILURE ...the Curse of the “SAFE” SYSTEM! —

Fault Tolerance is GOOD, as far as it goes  
...does it go as far as Common Causes?

- **DEFINITION** — A Common Cause is an event or condition which, upon occurring, induces malfunctions at *several points* within a system, producing system failure. The system may well have been designed to be invulnerable to *each* of those malfunctions, taken *singly*. But the Common Cause delivers a *double ding* ...or a *triple* ... or — and redundancy is defeated, *and the system crashes!*

- **EXAMPLES** — The most prevalent Common Causes are interruptions of *utility services*. **Think...**

**Electricity/Steam/Cooling Water/Pressurized Lube Oil/Compressed Air/...etc.**

Next come *environmental stresses* — e.g., the room temperature rise that kills the *primary* whatnot also takes out the *redundant backup* whatnot. **Think...**

**Moisture/Fire/Flooding/Heat/Freezing/Vibration/...etc.**

And *miscellaneous miscreants* are also numerous. **Think...**

**Vermin/Varmints/Mud Daubers/Human Operators/Software/...etc.**

### Common Causes are Redundancy Killers!

- **DIAGNOSIS** — How to *find* system vulnerability to Common Cause failures? Two methods prevail: (1) System inspection, and application of intuitive engineering skills; (2) Fault Tree Analysis, and a search for like sensitivity in all the terms in any Minimal Cut Set of the tree. (See Scrapbook Sheets 86-7 and 87-4.) *Awareness* of the insidious nature of the malady is essential to success by *either* means!

- **CURE** — *Avoiding* Common Cause failures rests on *preventing access* to the system, at more than a single *redundant element*, by the potential mechanism for inducing failure. This is done by providing redundant paths that are *not* sensitive to the Common Cause or by “separating” vulnerable system elements. The “separation” may be in space, in time, or in operating principle. **Think...**

**Relocate/Separate/Isolate/Insulate/Shield/...etc.**

AND

**Use Redundant Features with Dissimilar Operating Principles/Power Supplies/Readouts/...etc.**

*BOTTOM LINE*

*Common Causes* represent opportunities for *System Wipeout* by means that become too obvious, too late. *Sneak up on them before they sneak up on you!*

## — How far DOWN

## ...should a Fault Tree GROW? —

### WHEN IS A FAULT BUSH BETTER THAN FAULT KUDZU?

*Don't overdo a good thing!*

- **THE PROBLEM** — In Fault Tree Analysis, the analyst exploring contributors to that TOP undesirable event must choose the **system level** at which to cut off the analysis. Is the “stopping point” at *subsystems?* . . . *at components?* . . . *at set screws?* Analyzing too far down wastes resources. Stopping too early may sacrifice thoroughness. Too late burns analytical resources needlessly. The stopping point decision is best guided by the **purpose of the tree**...
- **NIFTY GUIDANCE** — Remember that Fault Tree Analysis is a Risk Assessment enterprise, and RISK has two components: SEVERITY and PROBABILITY. That **TOP** tree event statement must contain or imply a particular level of mishap SEVERITY. The function of the tree analysis then is to determine PROBABILITY and to display its sources within the system. Once probability has been established, the assessment of risk for the **TOP** is complete. Ergo, analyze the system down to levels no lower than is necessary to arrive at fault/failure events for which probability declarations can be made with reasonable confidence . . . whether that's the entire engine or the distributor cap. Then, propagate to the **TOP!**
- **SOME EXCEPTIONS** — Finer resolution — i. e., carrying the Fault Tree Analysis to lower system levels — is justified in two cases:
  - An alarmingly high probability is apparent for **TOP** or for a particular tree element. Analyze below that element to determine the **source(s)** of that big number and to find ways to **reduce** it.
  - A tree is being used to support an autopsy of a mishap. It may become necessary to explore the furthest reaches of the system to find the offending element(s) that caused the calamity.

#### *BOTTOM LINE*

Fault Tree Analysis is a valuable tool, but if you overuse it, it'll wear you out to no good purpose. *Don't analyze down to the submolecular level if you can stop earlier with the same risk assessment result!*

## — Using PEOPLE as COMPONENTS and... PROCEDURES as COUNTERMEASURES? —

*Great Gravy, don't count on them!*

Along with personnel come high probabilities of malfunxion!

- **THE PROBLEM** — Because *human operator* interactions with systems are commonplace, and because operating *procedures* are easy to invoke, *procedures* are often used as countermeasures to control the risk of system hazards. But the human operator, even when guided by checklists or written procedures, remains an imperfect system component. And operating procedures remain the *least effective* of all countermeasures. (See *Scrapbook Sheet 83-4*.)
- **EXAMPLES** — These typical operator error probabilities illustrate the phenomenon:
  - Operator omission of an independent step in a  
written procedure of 10 or more steps.....  $1 \times 10^{-2}$
  - Same as above, *with* check-off provision.....  $3 \times 10^{-3}$   
(Source: *NUREG/CR-1278*)

By comparison, the probability of failure-on-command for the average electronic circuit relay is of the order of  $10^{-4}$ . (Source: *WASH 1400*)

- **CAUTION** — Use human operators for *critical* functions when other methods are unavailable, are unworkable, or when you need a system component that thinks on its feet. *When* using human operators, recognize the finite, sometimes-high probabilities of error! Those probabilities can be *reduced* by imposing the discipline of checklists and procedures and by training and drilling. But they will remain high by comparison with failure rates for most non-human components.

### *BOTTOM LINE*

The human operator is irreplaceable at a system point where on-the-spot thought processes and decision making are musts. But people are imperfect components, and procedures don't make them that much better. *As fixed-function system components, people are poor performers!*

## — Fault Tree Diagnostic Tricks —

So, you've *grown* a Fault Tree? Now make it do *useful stuff* for your system!

- **PURPOSE** — Fault Tree Analysis evaluates *probability* of an undesirable outcome of system operation. So, it's a powerful *Risk Assessment* tool. You pick the nasty **TOP** event and identify its *severity*. The Tree gives you the *probability ...et voila: RISK!* Here are some useful Tree diagnostic aids...
- **Minimal Cut Sets** — These are least groups of Tree “initiators” that'll suffice to *guarantee* occurrence of the Tree **TOP**. They're sometimes *surprising* clusters of events/conditions! Better to be surprised by the *Tree* than by the *System!* Find the Cut Sets and work 'em. Locate the heavy hitters by computing Cut Set Importance. Build “intervenors” into the sick sets to raise reliability.
- **Path Sets** — These are least groups of initiators which, if they are *prevented*, will forever guarantee *no TOP!* Finding them can guide resource deployment to stomp System vulnerability.
- **“Parts Count”** — Need a quick look at an upper bound which  $P_{TOP}$  *cannot exceed?* Simply *sum* the P's for all the initiators. (This'll assume all Tree gates are **OR**'s — a “worst-case” diagnosis.)
- **“Suspicious” Initiators** — Worried about some *particular* initiator that's *buried* somewhere in the Tree? Unsure of its probability? Assign it some arbitrary value,  $P_{worrier}$ . Now, compute  $P_{TOP}$  with this nominal  $P_{worrier}$  in place. Then *recompute*  $P_{TOP}$  for a new  $P_{worrier2} = P_{worrier} + P_{worrier}$ . Examine the ratio  $P_{TOP} / P_{worrier}$ . This ratio is a crude measure of “sensitivity” of the Tree to that initiator. Rule of thumb: if this sensitivity exceeds 0.1 in a large tree, work to find a value of  $P_{worrier}$  having less uncertainty ...or, compute  $P_{TOP}$  for a  $P_{worrier}$  at its upper credible limit. If that  $P_{TOP}$  is unacceptable, you'd better get a “better”  $P_{worrier}$ !
- **Common Causes** — There's *no* easier way to uncover Common Causes than by subscripting the initiators with potential common-cause markers (e.g., H for human error, M for moisture, V for vibration, etc.) Then look at the cut sets. See a *solid row* with the *same subscript?* That'll be a Common Cause “hit!” To find its probability, see Scrapbook Sheet 87-4. And Scrapbook Sheet 86-4 deals with Common Causes.

### *BOTTOM LINE*

Finding **TOP** probability is only *one* cute Fault Tree trick. A buncha neat methods will help the Tree pinpoint System Vulnerability ...and help *you* improve The System. *Better a well-diagnosed Tree than a pranged system!*

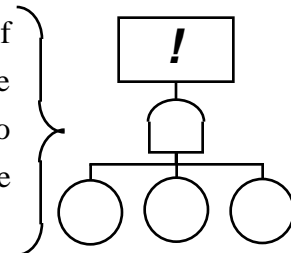
## — Growing a *FAULT TREE*? Selecting and Naming Faults/Failures is *IMPORTANT STUFF!*—

Rules of logic and probabilmism are easily violated by carelessly managed Fault Tree elements.  
Follow these simple rules to keep your Tree out of Trouble!

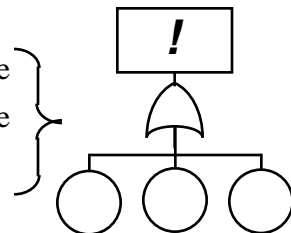
- Be *specific* in titling Faults/Failures. Say *exactly* what it is that faults or fails at a given point in the analysis logic, and in *what mode* ...e.g., “RELAY K-29 CONTACTS FAIL CLOSED”

- Once you’ve *titled* a Fault/Failure, use that *same title* for that *same event* wherever it appears in the Tree.

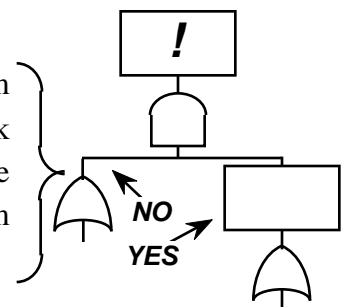
- Under an AND gate, as a *group*, the collection of Faults/Failures must be (1) *necessary* and (2) *sufficient* to serve as the *direct* cause of the event/condition at the AND output. Do not include any *unnecessary* elements. Make *sure* that the group *is* sufficient.



- Under an OR gate, *each individual* Fault/Failure must be sufficient *alone* to serve as the *direct* cause of the event/condition at the OR output.



- *Never* let a gate feed a gate. *ALWAYS* insert a system Fault/Failure statement in a box at each gate output to track Tree logic cleanly to the TOP! The statement should indicate what’s going on at that point in the analysis by way of system fault logic.



### *BOTTOM LINE*

Fault Tree Analysis is a tidy exercise in Symbolic Logic, aimed at finding System Vulnerability to Failure. But watch it! *If your Tree logic fails, then there’s no telling what your System might be up to!*

— FOUR OPTIONS are available...  
for *Managing RISK*  
...you're probably using several RIGHT NOW! —

You've got a system/process/mission/activity that poses too much risk for comfort. What to do? There are only FOUR CHOICES! ...consider them, and use one or more, as suits the occasion:

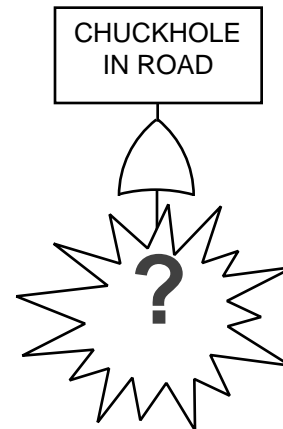
<u>OPTION</u>	<u>EXAMPLE(S)</u>
1. <b>REDUCE the risk</b>	Alter the <i>design</i> , or impose <i>engineered safety features</i> or <i>protective systems</i> or <i>warning methods</i> that suppress severity and/or lessen probability. (See Scrapbook Sheet 83-4 for Effectiveness Ranking of Risk Reducers.)
2. <b>AVOID the risk</b>	<i>Omit</i> the “risky” operation altogether, or <i>switch</i> to an alternate process, or material, or what-have-you.
3. <b>TRANSFER the risk</b>	Buy insurance, causing <i>others</i> to <i>accept the risk</i> , or get others to do the job by contracting it out. (Be sure to tell them what they're getting into — “failure to warn” carries heavy liability penalties.)
4. <b>ACCEPT the risk</b>	<i>Perform/operate despite</i> the recognized risk. (Biting the bullet is sometimes the <i>only</i> way to dispose of the nasty thing! Be sure those who bite the bullet know its caliber and powder charge!)

*BOTTOM LINE*

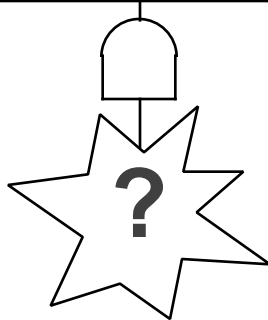
In managing RISK, consider the options, and select with care. *Ignoring risk is not an option. ...risk ignored is risk accepted by default!*

## — FAULT *TREE* turning into FAULT *KUDZU*? ...Scope that TOP EVENT! —

- **PROBLEM:** — Fault Tree Analysis is a powerful analytical technique. BUT if allowed to run amuck, it'll consume *many* manhours, to no good purpose. If the **TOP** statement is broadly drafted — i.e., too “general” — the Tree will take on *many* branches and twigs and will become absolutely asquirm with basic initiators! Many of these will be of little use in assessing risk of *the* event that *really* counts!



WHEEL ENCOUNTER WITH  
CHUCKHOLE DEEPER THAN 4 IN.  
AND LONGER THAN 10 IN. AT  
MORE THAN 12 MPH AND LESS  
THAN 48 MPH



- **CURE:** — Remember, that **TOP** statement represents the SEVERITY component of RISK! (The Tree aids in evaluating the PROBABILITY component.) Make that **TOP** severity statement a *tight* one. Are you interested, for example, in just *any* little bitty old FIRE, or a FIRE in a certain operation, resulting in more than a certain dollar/downtime loss? *Scoping* at the **TOP** will simplify the Tree and save lotsa time! To *scope*, use modifiers that *bound* the TOP statement. Limit stuff like time, space, place, circumstances, extent, etc. Stick to Severity Concepts!

### *BOTTOM LINE* —

Don't let your Fault *Tree* metastasize into a needless Fault *Forest*! A *little* care in writing the *headline* will go a long way toward shortening the story that follows!



## — Pondering Pranged Parts... and/or a Scrogged System? Here's a Whole Mess of *Neat Nomenclature!*—

You've probably got your *own* names for bazzracked hardware!  
Here's what the experts call it...

- **FAULT** — An abnormal *and* undesired state of a system or subsystem or component, induced by (1) presence of an improper command or absence of a proper one, or by (2) a failure. (See below.) All *failures* cause *faults*, but not all *faults* are caused by *failures*. (NOTE: Safety features which properly shut down a system have *not faulted*.)
- **FAILURE** — Loss, by a system, subsystem or component, of functional integrity to perform as intended. E.g., relay contacts corrode and will not pass rated current when closed, or the relay coil has burned out and will not close the contacts when commanded — that relay has failed; a pressure vessel bursts — the vessel has failed. (NOTE: A protective device which functions as intended — e.g., a blown fuse — has *not failed*.)
- **PRIMARY (or BASIC) FAILURE** — Failure in which the failed element has seen *no* exposure to environmental stresses or service stresses *exceeding* its *ratings* to perform. E.g., fatigue failure of a relay spring within expected lifetime; leakage of a valve seal under its rated pressure differential.
- **SECONDARY FAILURE** — Failure induced by exposure of the failed element to environmental and/or service stresses exceeding its ratings. E.g., the failed unit has been improperly designed or selected or installed for the application; the failed element is *overstressed/underqualified* for its burden.
- **Failed/Faulted SAFE** — Proper function is impaired or lost, but without further threat of harm. E.g., a pressure cooker “fuse” *opens* at *less* than rated pressure.
- **Failed/Faulted DANGEROUS** — Proper function is impaired or lost in a way which poses threat of harm. E.g., a pressure cooker “fuse” *does not open* above rated pressure.

### *BOTTOM LINE* —

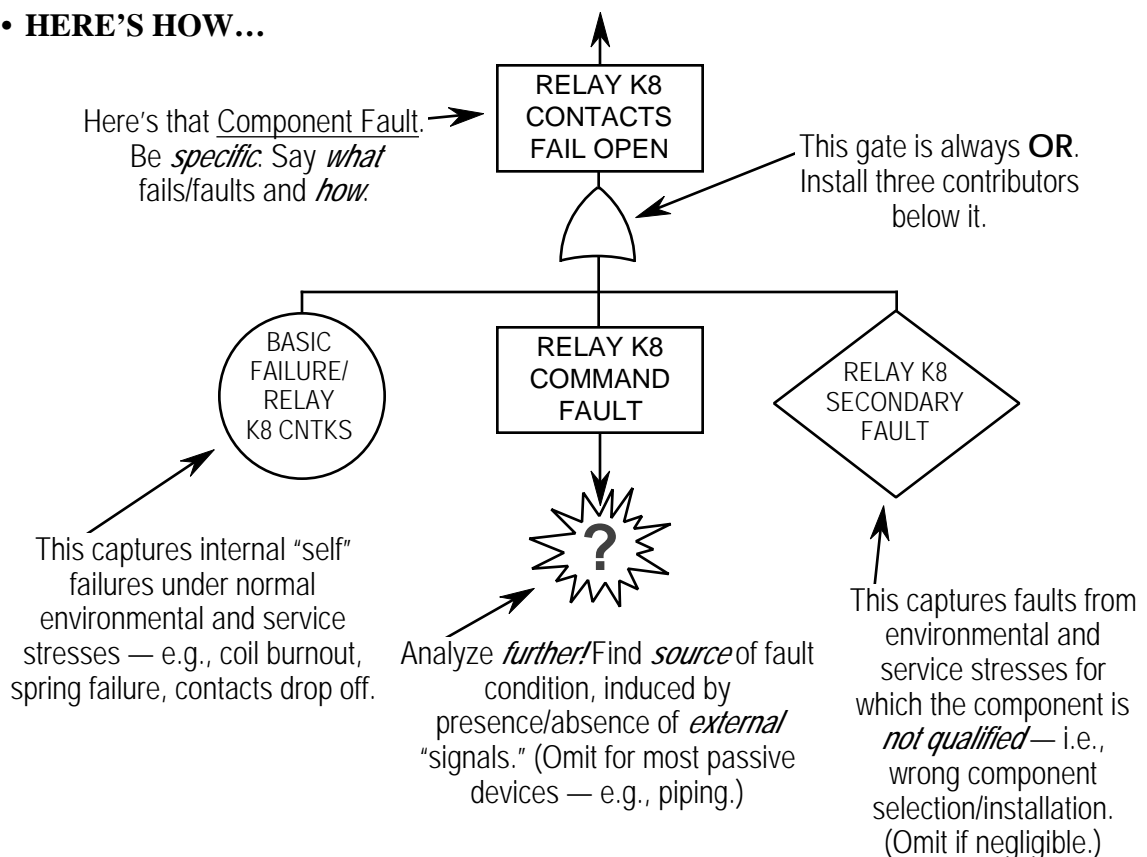
It's more important to analyze system *vulnerability* and to deal effectively with system *risk* than it is to call a system's crashes by elegant names ...*but keeping to common terminology sure helps communication amongst system analysts. The literature does it ...why not us?*

# — Has Your FAULT TREE arrived at a COMPONENT Fault? ...the STATE-OF-COMPONENT METHOD Can Help!

*Pre-thunk, Plug-in Logic Accelerates Analysis down there at the Device Level in Lotsa Systems...*

- **HERE'S WHY** — When a Fault Tree explores the potential causes and probability of a Big Nasty Event (**TOP**), analysis logic often sifts down through an array of system fault states to arrive at a level where contributors are *Component Faults*. (“Components” are discrete elements like valves, relays, pumps, transducers, pressure vessels, etc.) When the analysis reaches the component level and *needs* to go further (it may not *need* to — see Scrapbook Sheet 86-5), time can be saved and thoroughness ensured by using the State-of-Component Method (...from NUREG-0492).

- **HERE'S HOW...**



**BOTTOM LINE**

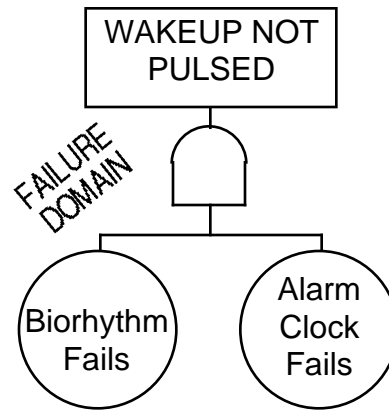
A system component induces a system crash (1) because it goes bust internally. (2) because other system elements mislead it, **OR** (3) because it's inappropriate to the job, and stresses catch up with it. *The State-of-Component Method makes for Automatic Fault Logic!*

## — Fault Tree Logic Looking Lumpy?

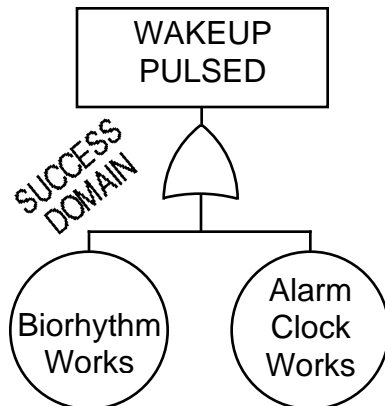
### Try the Flip-TOP Test to check it out! —

Loose-looking logic can be tested!  
Move it from the Failure to the Success Domain!

- **SYMPTOM** — Now and again, in analyzing a system using a Fault Tree, You'll encounter a hunk of system logic that just doesn't seem to "connect." You can't find anything *really* wrong with it, but it's got a loose look to it. Are *those* basic initiators *really* necessary and sufficient to produce *that* system state? Should that gate *really* be an AND? Attempts to "fix" it by editing and adjusting the logic seem to make it worse. *Don't* waste effort in jiggledy-poo adjustments. Try a simple duality flip...



- **DIAGNOSIS / CURE** — For reasons best called deeply obscure, *reversing* an argument in symbolic logic often makes it easier for the analyst to find flaws in its original form. (Remember that Fault Tree Analysis is just a symbolic method!) Simply *invert* every tree statement, and also reverse the gates, so ANDs become ORs and *vice versa*. The new "flipped" logic will tell the truth *if, and only if*, the original logic was properly constructed. (Students of Boolean algebra will recognize that this gimmick takes advantage of De Morgan's principle.) If the *new* tree looks silly, fix it and then *re-flip* it!



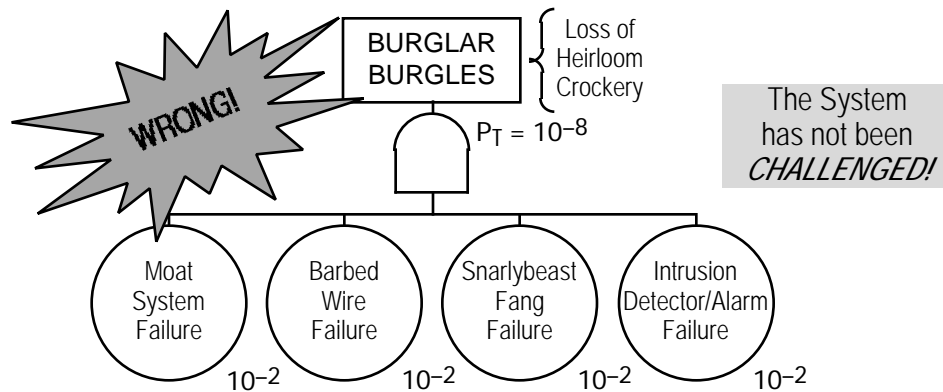
#### BOTTOM LINE

*Don't* waste effort arguing with a suspicious-looking Fault Tree. Mirror-image it into a *Success Tree*, and if it's still sickly, then it was *flawed to start with!*

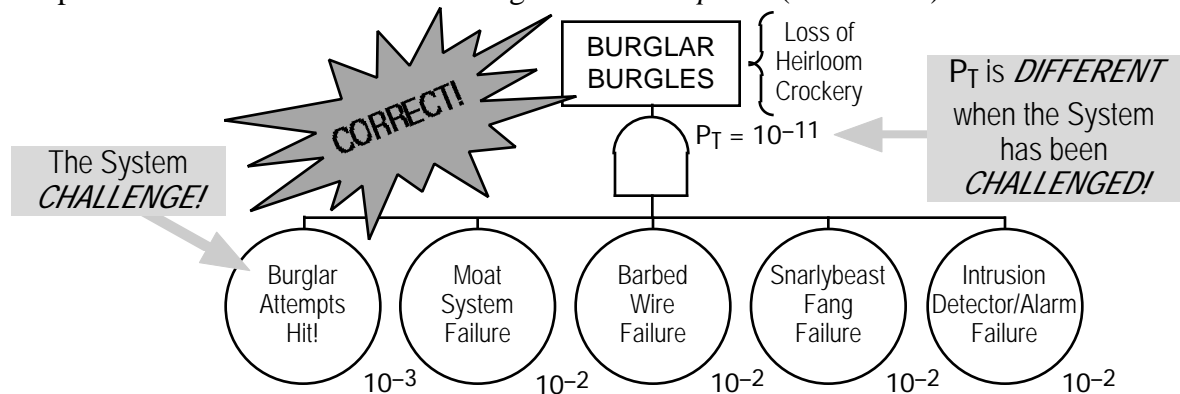
# — Assessing Risk for an ENGINEERED SAFETY FEATURE? ...Don't Forget the SYSTEM! —

Missing logic elements make for unrealistically high failure probabilities!

- THE SCROG-PROOF CRITICAL SYSTEM** — Safety Features protect many *critical systems*. Breakers protect circuits; pressure relief valves protect vessels; overtemperature shutdowns protect bearings ...intrusion preventers protect households. It's important to assess the *risk* of operating critical systems. *When* that risk is assessed, the countermeasuring effect of the safety feature(s) must be taken into account. The *severity* component of system risk — the *amount* of loss that would be suffered in a system crash — is usually easy to evaluate. The *probability* of a crash is the tough component to get at.



- AN ANALYTICAL GOOFATUNITY** — Too often, in such cases, the probability that a system's *safety feature(s)* will fail when challenged gets a nice exhaustive analysis, and *this* is taken as the probability of a system crash. (See above.) **BIG MISTAKE!** This *ignores* the probability that the safety feature will have been called upon — i.e., challenged — in the first place! The *real* probability needed for the system risk assessment is *not* the probability that the safety feature will fail when challenged, but the *conditional* probability that (1) there'll *be* a challenge AND (2) the safety feature will *then* fail in response to it. Make *sure* the whole logic trail is *complete!* (See below.)



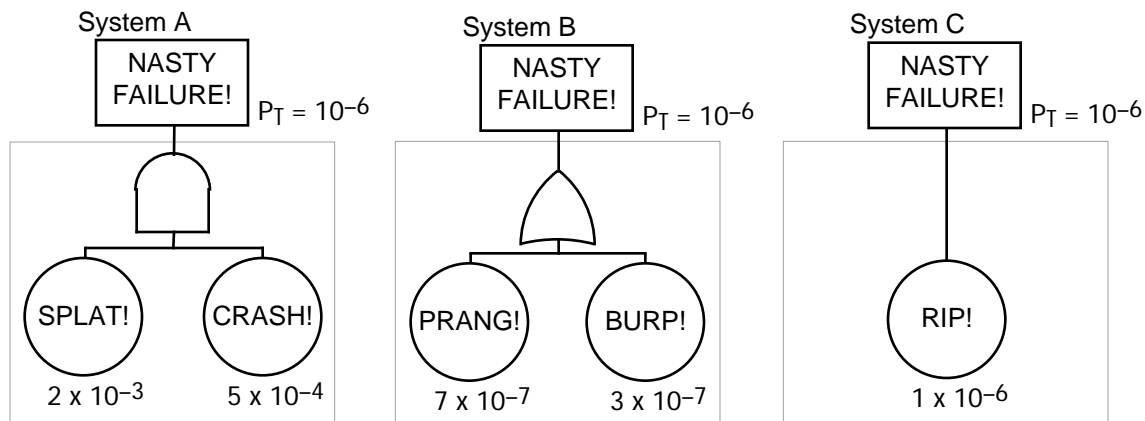
**BOTTOM LINE**

Have you *really* found the probability that you'll have a flat tire you can't recover from? ...or the probability that the jack won't work or the spare is sick when you need them? Safety features viewed *alone* may fail more frequently when challenged than the systems they protect ...does *your* analysis show this?

## — When Evaluating RISK Look-Alikes, Which System D'ya Pick? —

Severity's the same. Probability's the same. RISK's the same! What to do?

- **BACKGROUND** — From a group of competing shelf model candidates, you're picking a system to perform a given system function. Because *failure* to perform that function would result in *loss*, you're using Risk Assessment to guide the selection. And because *each* candidate would perform the *same* function, failure of any candidate would carry the same *severity* penalty. Apart from severity, risk has only one other component — **PROBABILITY!** So ...you do an innards analysis on the candidates to find the *probability* of failure, over the operational period of concern:



The system innards differ — “A” has redundancy, “B” has two potential single-point failures, “C” has only one potential single-point failure. But, the overall **TOP** failure probability is the *same* for *all*. Risk, therefore, is the *same* for the competing designs!

- **QUERY** — Now, which system do you *pick*?
- **ANSWER** — You pick the *cheapest* one (COST) that you can *get* (FEASIBILITY) on *time* (SCHEDULE).
- **CAVEAT** — When evaluating cost, don't overlook any of its parts: initial outlay / installation / operator training / operation / maintenance / decommissioning / ...etc.

### BOTTOM LINE

When evaluating competing systems, if failure severity and probability are the same for all, then *risk*'s the same, too, no matter *what's* inside the black box. Let cost decide the winner. *If a bunch of insurance policies offer the very same coverage, GO WITH THE CHEEPIE!*

## — *WHICH* System Safety Technique D'ya Use? ...and for *WHAT?*—

### *An Abbreviated User's Guide to a Few of the Many Analytical Methods*

There are *many* System Safety analytical techniques. Each has its own special strengths and shortfalls for a particular application. Here are some of the important bigees ...listed more-or-less according to prevalence of use:

- **PRELIMINARY HAZARD ANALYSIS:** A line-item tabular inventory of significant system hazards, and an assessment of the residual risk posed by each hazard in the presence of existing/planned countermeasures. Note: “Preliminary” is a misnomer. Although PHA is a “first-step” method, the hazard inventory can be prepared at any time in system life cycle and revisited, revised and enlarged as operating experience or system changes disclose new hazards or new information about old ones.

- **Where/When Applied:** Best applied commencing with formulation of system design concept, to cover whole-system and interface hazards for all operational phases. Applicable, however, at any time in system life cycle and to any portion of overall system.

- **Advantages:** Provides an orderly, useful log of all system hazards and their corresponding countermeasures. For uncomplicated systems, no further analysis may be necessary. Checklists are readily available to support the method — e.g., Scrapbook Sheet 86-1. (Scrapbook Sheet 96-2 is a Review Guide.)

- **Shortcomings:** Fails to assess risks of combined hazards or of system faults/failures which may co-exist. Thus, may lead analyst to false conclusion that overall system risk is tolerable simply because system risk is resolved into hazard elements each of which is acceptable, when viewed singly. (See Scrapbook Sheet 97-10.)

- **FAULT TREE ANALYSIS:** A top-down symbolic logic technique that models failure pathways within the system, tracing them from a predetermined, undesirable condition or event to the failures/faults that may induce it. Previous identification of that undesirable event (called **TOP**) includes recognition of its severity. The tree logic can ...more ➡

#### *BOTTOM LINE*

There are *many* System Safety analytical techniques. Some are mutually complementary, and some are redundant. Select the one(s) best suited to the job at hand. Identifying and controlling the threat of loss is the object of the System Safety game. *Learn your system's risks before your system teaches you what they are!*

be used to determine **TOP** probability. Thus, with severity and probability evaluated, risk assessment results.

- **Where/When Applied:** Particularly useful for high-energy systems (i.e., potentially high-severity loss events), to ensure that an ensemble of countermeasures adequately suppresses probability of mishaps. A powerful diagnostic tool for analysis of complex systems and as an aid to design improvement. Sometimes useful in mishap investigations to determine cause or to rank potential causes as to their probabilities. Applicable both to hardware and non-hardware systems.
- **Advantages:** Enables analysis of probabilities of combined faults/failures within a complex system. Identifies and analyzes single-point and common-mode failures. Identifies areas of system vulnerability and low-payoff countermeasuring, thereby guiding deployment of resources for improved control of risk. (Scrapbook Sheet 83-6 is a Review Guide.)
- **Shortcomings:** Treats only one undesirable condition/event. Thus, several or many tree analyses may be needed for a particular system. The undesirable condition/event is not disclosed by the analysis, but must be foreseen by the analyst. Deals awkwardly with sequence-dependent fault scenarios.

---

• **FAILURE MODES & EFFECTS ANALYSIS :** A bottom-up, tabular technique that explores the ways (modes) in which each system element can fail and which then assesses the consequences (effects) of each of these failures. Probabilities of individual failures can be entered, and risk for individual failure modes can be assessed.

- **Where/When Applied:** Applicable within systems and at system-subsystem interfaces. May be performed at any indenture level — i.e., subsystem, assembly, subassembly, component, or “parts-count” level.
- **Advantages:** Exhaustively thorough in identifying potential single-point failures and their consequences. (Scrapbook Sheet 84-1 is a Review Guide.)
- **Shortcomings:** Costly in manhour resources, especially when performed at the parts-count level within large systems. Applicable only *after* system elements have been identified — hence, later in design than may be desirable. Does not evaluate either the probabilities or the consequences of system failures induced by co-existing, multiple-element faults/failures within the system. Conceals whole-system risk. (See Scrapbook Sheet 97-10.)

- **EVENT TREE ANALYSIS:** A back-to-front symbolic logic technique that explores system responses to an initiating “challenge” and enables assessment of the probability of an unfavorable outcome. The system challenge may be a failure or fault, an undesirable event, or a normal system operating command.
  - **Where/When Applied:** Particularly useful in analyzing command-start/command-stop protective devices, emergency response systems, and engineered safety features. Useful also in evaluating operating procedures, management decision options, and other non-hardware systems.
  - **Advantages:** Multiple, co-existing system faults/failures can be analyzed. Can be performed quantitatively. Identifies and analyzes potential single-point failures. Identifies areas of system vulnerability and low-payoff countermeasuring, thereby guiding deployment of resources for improved control of risk.
  - **Shortcomings:** Treats only one initiating challenge. Thus, several or many tree analyses may be needed for a particular system. The initiating challenge is not disclosed by the analysis, but must be foreseen by the analyst. Although multiple pathways to system failure may be disclosed, the severity levels of loss associated with particular pathways may not be distinguishable without additional analysis.

---
- **ENERGY FLOW/BARRIER ANALYSIS:** An examination of all potentially harmful energy sources within the system, together with an assessment of the adequacy of safeguards for each to afford protection against unwanted release.
  - **Where/When Applied:** Best applied commencing with formulation of system design concept, but applicable also at any point in system life cycle and to any portion of the overall system. Of particular value as a means of developing a hazards inventory to support Preliminary Hazard Analysis. (Tabulation of the analysis and results may be done using PHA format.) Useful also in developing safe-entry procedures at disaster sites.
  - **Advantages:** A convenient, disciplined approach to cataloging energy-related system hazards. Checklists are readily available to support the method (e.g., System Safety Scrapbook Sheet 86-1).
  - **Shortcomings:** Hazards not directly related to unwanted energy release are often overlooked (e.g., confined space oxygen deficiency, pinch points and sharp edges).  
...more ➡



- **CAUSE-CONSEQUENCE ANALYSIS:** A back-to-front symbolic logic technique that explores system responses to an initiating “challenge” and enables assessment of the probabilities of unfavorable outcomes, at each of a number of mutually exclusive loss levels. The system challenge may be a failure or fault, an undesirable event, or a normal system operating command.
  - **Where/When Applied:** Particularly useful in analyzing command-start/command-stop protective devices, emergency response systems, and engineered safety features. Useful also in evaluating operating procedures, management decision options, and other non-hardware systems.
  - **Advantages:** Multiple, co-existing system faults/failures can be analyzed. Probabilities of unfavorable system operating consequences can be determined for a number of discrete, mutually exclusive levels of loss outcome. Identifies and analyzes potential single-point failures. Identifies areas of system vulnerability and low-payoff countermeasuring, thereby guiding deployment of resources for improved control of risk. Deals well with sequence-dependent fault scenarios.
  - **Shortcomings:** Treats only one initiating challenge. Thus, several or many analyses may be needed for a particular system. The initiating challenge is not disclosed by the analysis, but must be foreseen by the analyst.

---
- **SNEAK CIRCUIT ANALYSIS:** A topologic evaluation of a circuit to disclose design flaws capable of producing unintended system operation, or of inhibiting intended system operation, in the absence of component failures.
  - **Where/When Applied:** Applicable to electrical, hydraulic, pneumatic energy control and energy delivery systems. Best applied during detail design. Applicable as a post-failure autopsy technique to aid mishap investigation.
  - **Advantages:** Of value in aiding to ensure against design inclusion of unintended pathways for command, or for harmful release of energy, or for failure to transfer command or to release energy as desired.
  - **Shortcomings:** Heavy reliance on intuitive engineering skills. Necessary analytical reduction of circuit loops/branches to elemental topologic modules is costly in manhour resources, especially when performed for large, complex systems.

---

- **STRATEGY SELECTION:** A family of complementary probabilistic logic methods used to select a favored operating strategy or design option, affording minimum risk, from among a group of competing strategies/options.
  - **Where/When Applied:** Applicable to selection of operating procedures, system designs, management methods and technology research approaches. Applicable only after competing designs, methods, etc. have been formulated, but best applied before their implementation.
  - **Advantages:** Ensures selection of least-risk approaches from among competing options in cases where risk differences are apparently small or ill defined. A useful adjunct to cost-benefit analysis.
  - **Shortcomings:** Requires prior development of competing options and separate analysis of risk for each of them.

————— end —————

## — Doing a Preliminary Hazard Analysis? ...How D'ya *Find* the Hazards? —

A Preliminary Hazard Analysis is an inventory of system hazards and their risks. The PHA risk audit is often the *only* System Safety analysis that's needed for uncomplicated, straightforward systems. It's especially important that you've identified *all* of the hazards. Finding *all* of them is pretty hard to do. DO NOT rely on a *single* analyst or a *single* method! And at best, *you'll never find all of the hazards*. Here are assorted sources of help:

- Use intuitive “Engineering Sense.”
- Conduct physical inspections / examinations.
- Conduct real or simulated “Operational Walkthroughs.”
- Consider Codes / Regulations / Standards.
- Consult with / interview current or intended system users and operators.
- Use checklists — e.g., Scrapbook Sheet 86-1.
- Review prior System Safety studies for the same or similar systems.
- Review historical evidence, e.g.:
  - Mishap Files
  - “Near Miss” Records
  - “Lessons-Learned” Files
  - Quality Program Database
- Consider “external influences” — weather, temperature changes, seismography, etc.
- Consider “Operational Phasing” — See Scrapbook Sheet 86-3
- Consider “Common Causes” — See Scrapbook Sheet 86-4
- Use “Scenario Development” — i.e., “what-iffing.”
- Use Energy Flow/Barrier Analysis — see Scrapbook Sheet 87-1.

### *BOTTOM LINE*

There's much more art than science in assembling a hazards inventory for a system. It's a bit like a war game. And to win, you need all the help you can get. The purpose is to find the “enemy” hazards and assess the acceptability of the risks they pose *before* they find you!

**BEWARE:** *No PHA is ever complete!*

— So, You've Gone and Got Yourself  
*a Numerical Failure Probability!*  
 ...Now, Just What Does It *MEAN?*—

Now and again, in our practice of System Safety, we find it possible to work with objective *quantitative* values to express the probability of failure of components, subsystems, and such stuff instead of those subjective, qualitative probability expressions like “Occasional” and “Remote” that we more often use. And what emerges at the conclusion of the work is ...*voila*: A *NUMBER* representing the probability that mischance will prang our system during some specified interval of exposure. Oddly enough, a little numerical  $P_F$  can go a long way toward confusing the risk management issue. *How* do you judge the *acceptability* of a numerical probability, for a given severity level? It often helps to *compare* it to other numbers that represent risk-like phenomena. Here are a few generalized calibration points that may help you to bootstrap your way to risk acceptance decisions — all are based on one hour of exposure\*:

- $10^{-2}$  — Human operator error in response to repetitive stimuli.
- $10^{-3}$  — Internal combustion engine failure (spark ignition).
- $10^{-4}$  — Pneumatic instrument recorder failure.
- $10^{-5}$  — Distribution transformer failure.
- $10^{-6}$  — Solid state semiconductor failure.
- $10^{-6}$  — Motor vehicle driver/passenger fatality.
- $10^{-6}$  — Lifetime average risk of death by disease.
- $10^{-7}$  — Flanged joint pipe blowout (4-in. pipe).
- $10^{-14}$  — Earth's destruction by collision with extraterrestrial body.

---

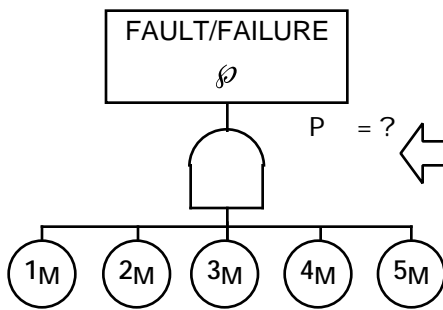
\*Source: R. I. Browning. “The Loss Rate Concept in Safety Engineering.” 1980

*BOTTOM LINE* —

Quantitative probability analysis is *great* stuff! BUT ...make sure the numbers you're using make real sense in the real world. AND ...watch out for little bitty system failure probability numbers like  $10^{-28}$ . *They* probably mean that something has been *overlooked* in the analysis — like a total wipeout of the planet where your system lives!

— So, you've found a **COMMON CAUSE!**  
 ...now how do you *Analyze its Effect?*  
 An OR gate can be your Best Buddy ...for once —

You've gone and grown a Fault Tree, and you've done a Common Cause search, using the Minimal Cut Set subscribing method. (See Scrapbook Sheets 86-4 and 86-7.) And *now* you've found that you've got a full cut set wipe-out, on a *single* Common Cause. AND (here's the real scary part) that Common Cause is *not* represented anywhere in your entire, fully grown tree ...*Oh, groan!*

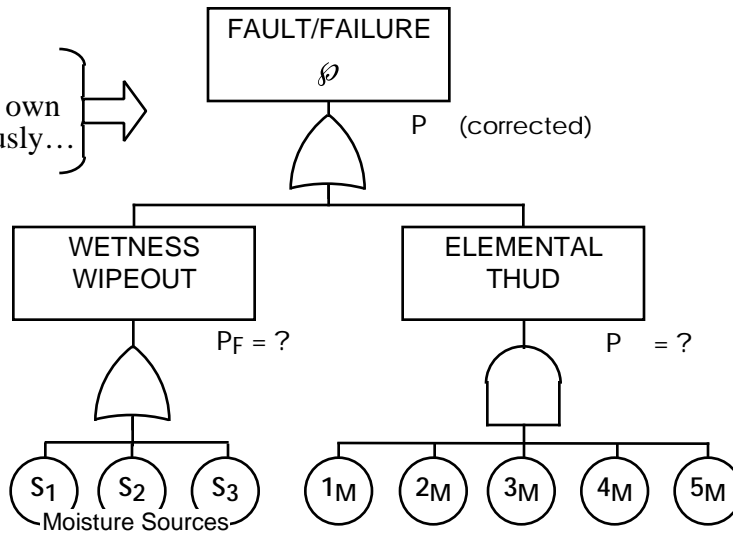


Here, the Common Cause M (Moisture, let's say) is found to be a full-branch killer that'll dump the whole Cut Set. Barring divine intervention, it'll corrode the switch contacts 1<sub>M</sub> and short the PC board 2<sub>M</sub> and flame-proof the lamp wick 3<sub>M</sub> and bazzrack its way through *all* the initiators to give the system a full case of the  $\phi$  nastiness. *UGH!*

So ...whaddy'a do *now?*

**STEP ONE:** Do *not* re-do the whole danged tree!

**STEP TWO:** Represent the Common Cause and its own P<sub>F</sub> using an OR gate, thusly...



Each moisture source S<sub>1</sub>-S<sub>3</sub> is represented at its probability of knocking down 1<sub>M</sub> thru 5<sub>M</sub>.

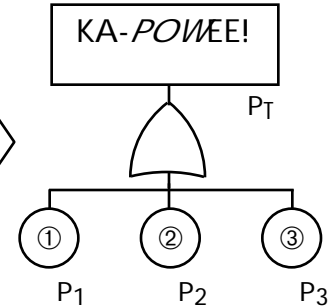
**STEP THREE:** If you *can't stand* the new P that you get outta this *proper* analysis, then you'd *sure* better get one or more of those components 1-5 outta that moisture!

**BOTTOM LINE**

Common Causes are commonly *overlooked* and commonly *underanalyzed*.  
 Don't let an undiscovered, unanalyzed Common Cause prang your system!

## — Need Probability for *Rare* OR-Gated Events? ...then use the *Rare-Event Approximation*—

- **THE EXACT MESS** — You’ve got an array of system elements for which failure is modeled thusly. And you’ve got trustworthy values of  $P_{\text{Failure}}$  for the three initiators. And they are statistically independent — i.e., if ① occurs, it neither induces ② nor precludes ② from occurring, and so on...



The Exact Solution for  $P_T$  is a squirmy mess, even for this trivial case:

$$\begin{aligned}
 P_T &= P_1 + P_2 + P_3 \\
 &\quad - P_1 P_2 - P_2 P_3 - P_1 P_3 \\
 &\quad + P_1 P_2 P_3
 \end{aligned}$$

And *that's* just for three initiators. For *four* initiators, we're into 15 terms in this messy expression!

- **THE TIDY APPROXIMATION** — Don't do it that way unless you *have* to. And, if those individual  $P$ s are small, you *don't* have to! Drop those fussy “exclusion” terms, leaving just...

$$P_T \approx \sum_{i=1}^{i=n} P_i = P_1 + P_2 + P_3 + \dots + P_n$$

This is the *Rare-Event Approximation*. If Events  $1 \dots n$  are Mutually Exclusive, it's also the *Exact Solution*.

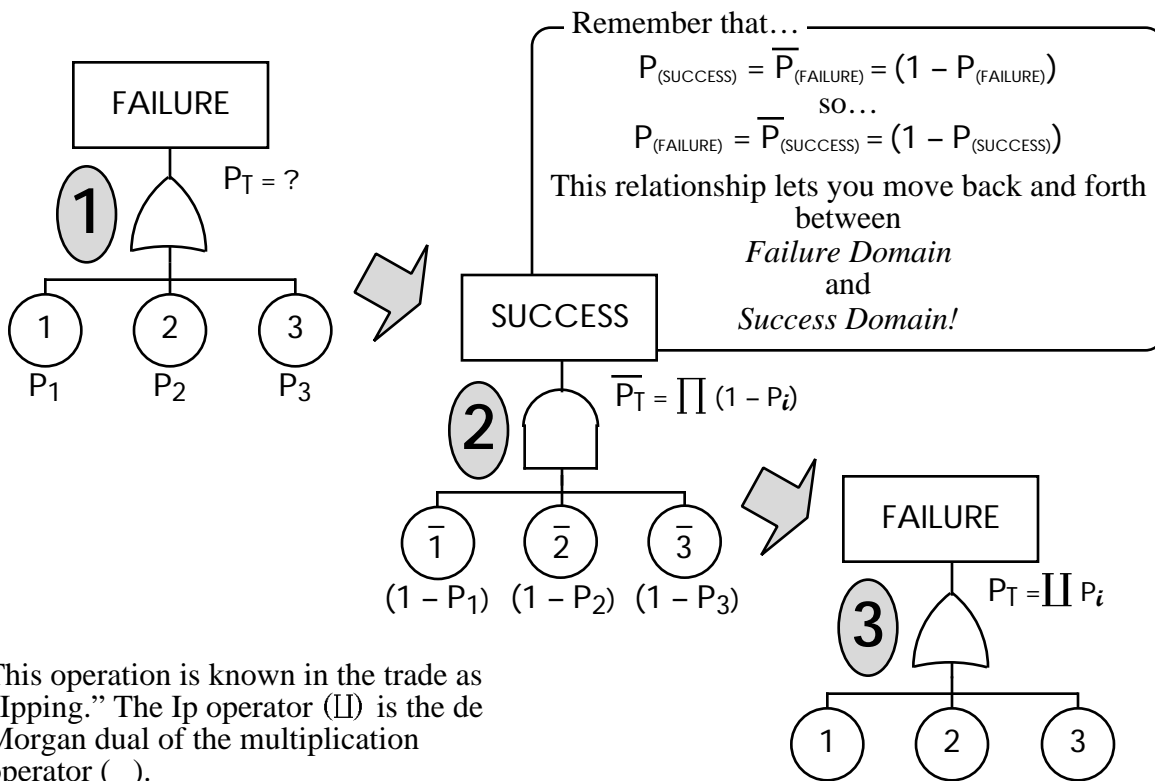
- **A NIFTY EXAMPLE** — Let's suppose, for example, that the  $P$ s for those three initiators are small, at values  $P_n = 0.1$ . (That 0.1 is *not* very “rare,” but it'll illustrate the point.) That'll give a  $P_{\text{EXACT}} = 0.271$  ...and  $P_{\text{APPROX}} = 0.3$  ...a difference of only 11%. That's *plenty* close enough in this line of work, where even the best numbers are lumpy! ALSO, notice that  $P_{\text{APPROX}} > P_{\text{EXACT}}$  ...which keeps the analysis just a skootch *pessimistic*, and **THAT'S GOOD!**

### BOTTOM LINE

If you've got small  $P$ s, like 0.1, and you're going through an OR, simply SUM 'em. And, *if you've got  $P$ s much bigger than 0.1, you don't need a Rare-Event Approximation — you need a new system!*

# — *Can't Stand* the Rare-Event Approximation? ... "Ip" your way to an *Exact Solution!*—

You're analyzing your way around out there in Failure Domain, where the Fault Trees grow, and you've got a bad case of the OR-gate high  $P$ 's. Or, for some *other* crazy reason, you really *do* need an *exact* OR solution. So ...the Rare-Event Approximation just won't work. (It's that thing back there on Scrapbook Sheet 87-5.) There's a *swift* way to get an exact solution without using all those pesky old exclusion terms. Do it by flipping from failure domain to success turf, where OR becomes AND, and propagate through AND by simply multiplying. Then shift back to failure space for the exact value of  $P_T$ . This uses the de Morgan "flip-top" gimmick from Scrapbook Sheet 86-13.



This operation is known in the trade as "Ipping." The Ip operator ( $\overline{\overline{\quad}}$ ) is the de Morgan dual of the multiplication operator ( $\prod$ ).

Thus, the *Exact Solution* is:

$$P_T = \prod_{i=1}^n P_i = 1 - \overline{P}_T = 1 - \prod_{i=1}^n (1 - P_i)$$

$$P_T = 1 - [(1 - P_1) (1 - P_2) (1 - P_3) \cdots (1 - P_n)]$$

← This works for Failure Domain propagation through OR's.

**BOTTOM LINE**  
Don't add BIG  $P$ 'S through an OR with the expectation of success.  
*The Rare Event Approximation only works for Rare Events!*

## — I've got *Reliability* data... ...so how do I get *Probability of Failure*? —

*A little bit of arithmetic provides a wealth of useful information for the Harried Analyst!*

- **The Problem** — Reliability Engineering predates formal System Safety Practice by several decades. Good reliability data bases go back at least as far as the early 1950s, and there are now gobs of them. So, you'll often be able to get reliability data for your system's innards when what you really want are data representing failure probability.

Lapse not into despair — *help is on the way!*

- **Some Definitions** — Let's divide the total ( $T$ ) of all attempts at an operation (or intended hours of operation) into those for which it succeeds ( $S$ ) and those for which it fails ( $F$ ). So...

$$S + F = T$$

Let's then define *failure* probability as...  $P_F = \frac{F}{T}$

And we'll define *success* probability, which *is* reliability ( $\mathcal{R}$ ), as...  $\mathcal{R} = \frac{S}{T}$

- **Addition** now gives us...  $\mathcal{R} + P_F = \frac{S}{T} + \frac{F}{T} = \frac{S+F}{T} = \frac{S+F}{S+F} = \mathbf{1}$  } An outcome of enormous convenience!

- **So Subtraction** gives...  $P_F = (1 - \mathcal{R})$
- **Watch out!** — Make sure that the exposure interval for  $\mathcal{R}$  matches the interval for which you want  $P_F$ . If it doesn't match, then adjust it!
- **A Limitation** — All of this is based on the presumption that reliability and failure probability are complementary. And they *are* complementary... mostly. But the kind of failure the System Safety Practitioner is interested in isn't just *any* old failure — it's a *subset*...it's only those failures that *induce loss*. So this method will give a failure probability that's exact only if all failures yield losses. For all other cases, it'll give a probability value that's a skootch high — i.e., *pessimistic*. And if you've gotta err in this line of work, do it pessimistically!

See, also, Scrapbook Sheet 02-2

### BOTTOM LINE —

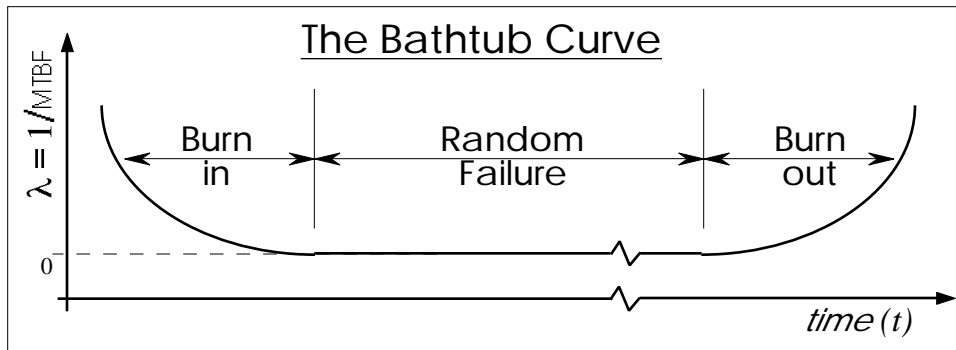
An apparent dearth of failure probability data may be nothing more than a great opportunity to exploit the numbers from a reliability handbook. Try a little simple subtraction before moving into irrational despondency!



## — The *BATHTUB CURVE*... ...handy Modeling of Life Failure Likelihood —

It can be very useful to have a long-term view of failure probability as a function of whole-life duration!

- **For many classes of system elements, and systems themselves**, the plot of long-term failure rate as a function of time has the appearance of the cross section of an old-fashioned Duncan Phyfe bathtub. At the outset of item life, there's a relatively high probability of failure, measurable as the reciprocal of Mean Time Between Failures (MTBF). Failure rate diminishes during this “Burn in” or “Infant Mortality” phase, and then becomes constant for a lengthy period of useful system life during which failures occur randomly, but at a long-term rate that is constant. At the end of this flat bottom of the bathtub, the average failure rate rises in a “Burn out” phase of system life, sometimes called “fatigue failure” or “wear out.”



- **The Bathtub Curve** is a very useful model of lifetime failure probability for many items — cars, toasters, solenoid valves, relays, humans — but...*BE CAUTIONED!* There are some pretty important things that the bathtub curve does NOT apply to, at all. In some cases, for example, Burn in occurs as a part of manufacture. (Burn in is still there, but the user isn't inconvenienced by it.) Or Burn in may be avoided by robust design and zealous manufacturing quality control. And Burn out can sometimes be postponed by energetic maintenance, inspection, testing, and parts replacement. Then, there's SOFTWARE, which does not emerge from random failure and enter Burn out. (You've probably worked with software that's never even emerged from Burn in!)
- **Notice that  $\lambda_0$** , the value of  $1/MTBF$  at the flat bottom of the bathtub curve, can be adjusted by varying the level of maintenance and the other random-failure “extenders” mentioned above.

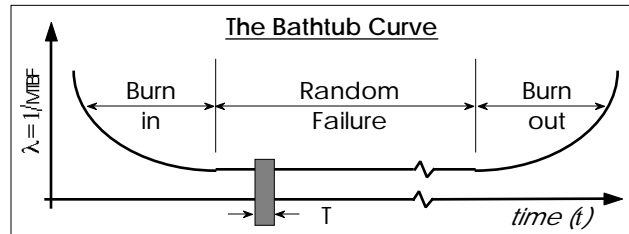
### *BOTTOM LINE*

Think about *your* system — can you “park” it on the flat bottom of the bathtub curve at a value of  $\lambda_0$  that's low enough, and then *keep* it there? *That's what risk management is all about!*

— WATCH OUT for MTBF...  
 ...it does *not* mean “Life Expectancy” —

*An MTBF is not a warranty!*

- **Mean Time Between Failures (MTBF)** is a term that’s a lot more often used than it is understood. If, for example, we learn that the **MTBF** for a component or a system is 77 years, we might expect that it’ll probably do just fine for at least 65 years or so, and then with each succeeding month it’ll stand an increasing chance of poodling out. *NOT SO!* Let’s assume that the item operates on the flat bottom of the



bathtub curve. That’s where **MTBF** is constant. It’s where most stuff works, most of the time. Failure probability for such a system can be modeled according to the simple exponential function...

$$P_F = 1 - e^{-T} \left\{ \begin{array}{l} \text{where: } T = \text{exposure interval} \\ \quad = 1/MTBF \\ \quad = \text{Napierian base (2.718...)} \end{array} \right\} \quad \left. \begin{array}{l} \text{See Scrapbook} \\ \text{Sheet 97-3} \end{array} \right\}$$

Now let’s evaluate  $P_F$  for an exposure interval of one month during any one of those 77 years — pick just any old month:

$$P_F = 1 - e^{-\left(\frac{1}{12 \times 77}\right)} = 0.001$$

So...the probability of failure during a one-month interval is 0.001, or 0.1%. It doesn’t matter whether that’s the *first* month or the *900<sup>th</sup>* month. The **MTBF** is *constant*, remember? It only gets that way if the failure probability is constant. That’s what the flat bottom of the bathtub curve is all about. And if you’ve got a fleet of 1000 of these things, one of them will poodle out each month, on average.

- **But** what if **MTBF** isn’t constant? *Well...* then we’re not on the flat bottom of the bathtub curve anymore, are we? And so we can’t claim a constant 77-year **MTBF**.
- **How do we stay on the flat bottom?** — Shrewd use of robust maintenance, inspection, testing, parts changeout, and other “renewal” measures will let us both *adjust* the value of **MTBF** *and* keep it constant, postponing the arrival of burn out.

*BOTTOM LINE*

The roulette wheel that only produces a win an average of once every 1000 spins doesn’t wait until around the 980<sup>th</sup> spin to begin thinking seriously about winning!

— ***“SCOPING” is a MUST***  
**...to keep *THOROUGHNESS* under control —**  
*It matters HOW MUCH SYSTEM you analyze!*

**WHEN DOING A SYSTEM SAFETY HAZARD ANALYSIS/RISK ASSESSMENT** by any of the many techniques available\* it's important to designate exactly what you WILL and what you WILL NOT cover. Where does the “system” start and stop? Consider bounding the analysis — i.e., specifying the extent of the analysis according to elements like...

- **PHYSICAL BOUNDARIES** — Where does the analysis begin and end? Perhaps you're analyzing everything downstream of Valve A-26 and west of Line G-G, except for the controls? Describe the limits in terms of geography and/or system architecture.
- **OPERATIONAL PHASES** — Is “Startup” to be considered along with “Standard Run?” How about “Emergency Shutdown?” ...and “Calibration?” ...and “Maintenance?” Say *which phases* apply! (See Scrapbook Sheet 86-3.)
- **INTERFACES** — Will subsystem-to-subsystem links be treated? ...i.e, you're doing the radiator and the fan and the water pump — will you consider the fan *belt*? ...or not?
- **UTILITIES** — Will compromises or outages of electricity / water / compressed air / gas / steam / etc. be considered or ignored in the analysis?
- **OPERATOR ERRORS** — Is the human operator “in” or “out” of the analysis? If “in,” are prudent standards of operator training and discipline assumed? (Such assumptions *don't* give an *error-free* operator!) Don't leave doubt — spell it out!
- **CODE CONFORMANCE** — Will you assume that the system conforms to applicable codes/standards? (That assumption doesn't make the system perfect!)
- **“TRIVIAL” HAZARDS** — Will you exclude “trivial” hazards? — i.e., those obviously in the lower left corner of the risk assessment matrix.

---

\*For scoping as it applies to Fault Tree Analysis, see also Scrapbook Sheet 86-10.  
Scrapbook Sheet 01-3 deals with “Exclusions,”  
Scrapbook Sheet 01-4 with “Assumptions,”  
and 01-6 with “Limitations.”

***BOTTOM LINE***

It's *great* to analyze thoroughly, but be sure to say what it *is* that's *getting* the thorough analysis. It'd better be something less than the entire solar system and its total contents during all operational phases including Startup and Emergency Stop!

## — Preliminary Hazard Analysis Review Hints —

*...so you've done a PHA — has it done these things?*

- Has the System to be analyzed been defined/bounded/scoped? (See Scrapbook Sheet 96-1.)
- Has a Probability Interval been declared? (See Scrapbook Sheet 84-4.)
- Have Operational Phases been recognized/differentiated? (See Scrapbook Sheet 86-3.)
- Are Human Operator error-induced hazards accounted for?
- Are Interface Hazards accounted for?
- Are Utility/Support Subsystem Hazards accounted for?
- Are Hazard Titles and Descriptions unique, or are there duplications/overlaps?
- Do Hazard Descriptions indicate source, mechanism, outcome? (See Scrapbook Sheet 98-1.)
- Is the Severity Component of risk consistent with the worst credible outcome?
- Is the Probability Component of risk consistent with severity at the worst credible level?
- Are target-to-target differences in the probability component of risk rational?
- Is the Probability Component of risk consistent with the record of experience?
- Has an assessment of Residual Risk been made for the system *after adopting* new countermeasures?
- Do the Indicated Countermeasures actually reduce severity and/or probability, and by the amount(s) shown?
- Do the Indicated Countermeasures introduce new hazards? (If so, are they represented?)
- Do the Indicated Countermeasures unreasonably impair system performance?

### *BOTTOM LINE*

Preliminary Hazard Analysis gives a whole-system inventory of all system hazards.

Make sure it tells how big is *whole* and how much is *all*.

## — The Thorough Analyst's Penalty —

*...the price of being good can be NO Operation!*

- **SYSTEM “A”** has been designed and built and is ready to be installed and operated. A System Safety study was begun at the outset and has accompanied the whole effort. A final report on the study has been submitted and has described all of the identified hazards and the countermeasures implemented to control their risks. The System Safety study has shown that for all of the hazards, risk is under adequate control. A total of 2187 hazards have been identified in the study. (The team performing the analysis has been exhaustively thorough.)
- **SYSTEM “B”** competes with “A” and is intended to do the same job. It is also ready to be installed and operated. As with “A,” a System Safety study has accompanied the “B” effort. A final report on the study has been submitted and has described all of the identified hazards and the countermeasures implemented to control their risks. The System Safety study has shown that for all of the hazards, risk is under adequate control. A total of 127 hazards have been identified in the study, which was performed during the late afternoon of the day before it was submitted. (The team performing the analysis has done a slapdash job.)
- **WHICH SYSTEM** is picked for installation and operation? — “B,” of course! The superficial appearance is that “A” is more than ten times “riskier,” because it has 17.2 times as many hazards. *And* because those making the decision have not been informed of the differences in thoroughness separating the “A” and “B” analyses. (Notice that “A” and “B” may even be identical systems!)
- **WHAT WENT WRONG?** — No one bothered to question the degree of thoroughness that characterized *either* analysis. With the presumption that they were equally thorough, which system would *you* have picked?
- **HOW TO PREVENT IT!** — Make certain your analysis report describes your degree of thoroughness. How much system did you analyze and how much did you omit? (See Scrapbook Sheet 96-1.) What methods did you use to *find* the hazards? (See Scrapbook Sheet 87-2.) What assumptions did you make? Did you include or exclude consideration of the human operator, for example?

### *BOTTOM LINE* —

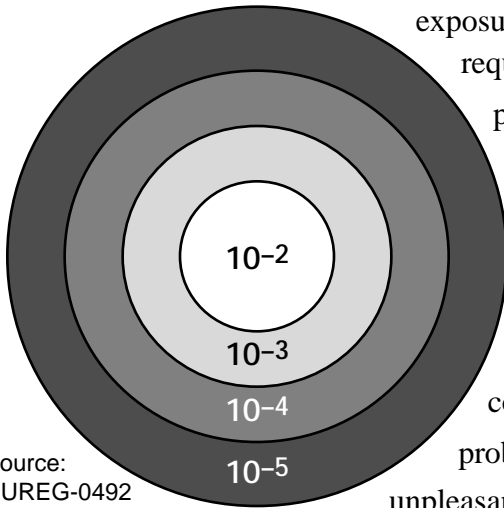
Too much of a Good Job can get you *nowhere*, unless the boss knows what it's all about.

*BE SURE HE KNOWS!* That's part of your Good Job, too!

## — Leapfrog Countermeasuring too often Deludes the Analyst —

*...pacifying large varmints promotes lesser varmints to bite you!*

- REQUIREMENT** — Let's suppose that our system design guidelines demand that there must be no hazards having probabilities of  $10^{-3}$  or greater of producing losses during the exposure interval that is of concern. To meet this requirement, we identify all hazards having probabilities  $10^{-3}$ , and then to reduce their probabilities, we impose redundancy — a designer's natural response to such a requirement. For these hazards, the probabilities of producing a mishap are now of the order of  $(10^{-3}) \times (10^{-3}) = 10^{-6}$ . A sense of comfort follows. We may now conclude that we have no nasty hazards with probabilities greater than  $10^{-6}$  of producing unpleasantness.



Source:  
NUREG-0492

- WHOA!**...Don't be bamboozled! What about some of those hazards that we ignored in the original search because they were *just* out of bounds? ...those with probabilities of  $10^{-4}$  or  $10^{-5}$ ? Now *they* will rise up to cause us whatever grief we may suffer! — and with probabilities one or two orders of magnitude greater than the ones we've dealt with!
- CURE** — After setting a risk tolerance threshold for a design and limits of resolution and boundaries for an analysis, it's as important to be mindful of the system elements that scoping has *excluded* as it is to work with the ones that have been *included*!

### *BOTTOM LINE*

Driving all the demons from under the sink does not result in having no demons to cope with. A demon that was in the basement and thought to be less threatening now becomes a lousy nuisance!

— Requiring low failure probabilities is *one* thing  
 ...proving you've *got* them is yet *another!*—

*...the lust for little-bitty numbers is too often fraught with unreasonableness!*

How often have you heard that a component or a subsystem or a system has or must have a failure probability no poorer than, say,  $10^{-7}$  per hour? ...and it must be demonstrated ...and there's scant or zero data from which to evaluate  $P_F$  ...and, ...well, you can name some of the other constraints.

***Just how reasonable are such expectations?***

As a test of reasonableness, have a look at this sobering table showing the number of no-failure empirical trials necessary to support claims of failure probability at various values, all of them higher than  $10^{-4}$  ...and that's pretty high:

For 95% Confidence	There must be <b>NO FAILURES</b> in...	to give Failure Probability $P_F \approx \dots$	which means Reliability $R \approx \dots$
<b>ASSUMPTIONS:</b> • Stochastic system behavior • Exponential failure distribution • Constant system properties • Constant service stresses • Constant environmental stresses	<b>1000 trials</b>	<b><math>3 \times 10^{-3}</math></b>	<b>0.997</b>
	<b>300 trials</b>	<b><math>1 \times 10^{-2}</math></b>	<b>0.99</b>
	<b>100 trials</b>	<b><math>3 \times 10^{-2}</math></b>	<b>0.97</b>
	<b>30 trials</b>	<b><math>1 \times 10^{-1}</math></b>	<b>0.9</b>
	<b>10 trials</b>	<b><math>3 \times 10^{-1}</math></b>	<b>0.7</b>

Source: Any Reliability Engineering textbook.

Before you make a claim that you've achieved a  $P_F$  of  $10^{-3}$ , or before you let someone impose a  $P_F = 10^{-3}$  requirement on you, stop and think — to support the claim at the 95% confidence level, that means 3000 trials without one failure. Is that *reasonable* for the case you have?

See, also, Scrapbook Sheet 02-3

***BOTTOM LINE***

For  $P_F = 10^{-9}$  / hour, MTBF for a full-time (24-hr/day) system  $\approx 114,000$  years.

If you can't *measure* it, think twice about *asking* for it.

You'll never know whether you've got it or not!

## — When *Probabilities* are *Challenged*, Here are some *Ploys to Pursue* —

*Well*, now ...you've done your *very* best at assessing probability of failure, either quantitatively or subjectively. And *now*... you find that Important Folks dispute your  $P_F$ . So ...it's important to respond. Here are some hints on how:

- **CITE SOURCES** — Make sure the sources / origins / methods used in arriving at your probability declarations are all documented and well understood. Always cite sources for handbook values, and always explain selection and use of modification factors. If you use engineering estimates, name the engineers and give dates.
- **QUESTION THE CHALLENGER** — The challenger of a failure probability declaration must have an alternate value and/or assessment method in mind. Without being provocative, probe the basis for the differing viewpoint. Don't be satisfied with an answer that simply says, "...your value is too high! (or too low)" You deserve to know the technical reasons *why* it's too high (low). Those reasons must be sound ones!
- **REASONABLE-MATCH COMPARISONS** — Do "reasonableness tests" to show how your value compares to handbook or actuarial failure probabilities for comparable phenomena.
- **"NO-FAILURE" COMPARISONS** — Remind your challenger of the number of no-fault tests required to justify 95% confidence in  $P_F$  at any probability level. (See Scrapbook Sheet 97-1.) The comparison is often jarring!
- **INVITE CO-AUTHORSHIP** — Always indicate the sources for all probability declarations in the text of your analysis report or in an attached table. If your challenger differs, invite him to contribute to the table with the understanding that he'll then be listed as a source for whatever probability declarations he introduces.
- **OBJECTIVITY** — Keep an open mind — there's always the off chance that your challenger knows something you don't!
- **AVOID ADVERSARIALISM** — Don't be argumentative. Contentiousness will get you enemies rather than a resolution of whatever problem you may be having with probability.

### *BOTTOM LINE* —

When a higher-up dislikes your version of the low-down on the odds, get him to participate in the oddsmaking ...and make him a co-author of the book!



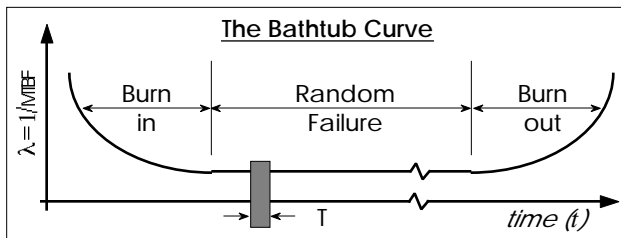
— I've got MTBF...so now,  
how do I get  $P_F$  for a short (or long) interval? —

*Linear scaling is OK, sort of, unless...*

- **When Exposure is BRIEF** ( $T < 0.2$  MTBF), then simple linear scaling gives failure probability ( $P_F$ ) within about 2% ...accurate enough for all but very rare purposes:

$$P_F \approx \lambda T \quad (\text{where } \lambda = 1/\text{MTBF}, \text{ and } T = \text{exposure duration})$$

This is called a “rare-event approximation.” For longer exposures ( $T > 0.2$  MTBF) it gives increasingly pessimistic values for  $P_F$  ...i.e., its errors over-approximate  $P_F$ .



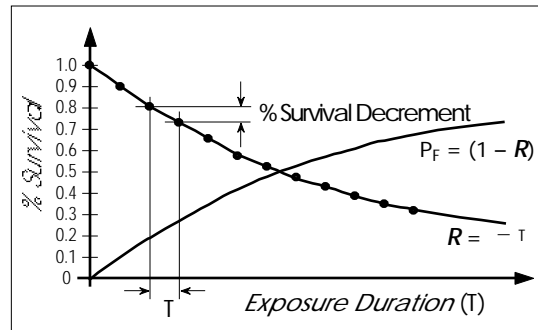
- **BUT...if Exposure is LONG**, then a more exact solution is needed. Remember the Bathtub Curve (Scrapbook Sheet 95-2). On the bathtub's flat bottom where is constant,  $T$  is exposure interval. Its width can be varied. ( $T$  must not be

confused with ongoing time,  $t$ .) As  $T$  is incrementally widened ( $\Delta T$ ), the probability the system will survive throughout  $T$  decreases.

This probability decreases by an equal *percentage* for each equal incremental increase in the width of  $T$ . So... it can be represented by an exponential function that is its own derivative. This function is *Reliability (R)*:

$$R = e^{-\lambda T} \quad (\text{e is the Napierian base, } 2.718^+)$$

Now, from Scrapbook Sheet 95-1, remember that  $P_F = (1 - R)$ . So...



$$P_F = (1 - e^{-\lambda T})$$

- **Let's try this on a PRACTICAL CASE** — Suppose our system has a Mean Time Between Failures of 500 hrs. We intend to operate it for 200 hrs, far more than 0.2 MTBF. (Notice that  $\lambda T = [(1/500) \times 200] = 0.4$ . This would be the value of  $P_F$  using the rare-event approximation.) Let's evaluate the probability of failure during the 200-hr exposure...

$$P_F = (1 - e^{-\lambda T}) = (1 - e^{-0.4}) = 0.33$$

Thus, for this case, the rare event approximation would err pessimistically by 21%.

**BOTTOM LINE**

If exposure duration is *short* compared to an MTBF, do it the easy  $\lambda T$  way. But if exposure is *long*, use the exponential solution unless you can stand a whole mess of pessimism!

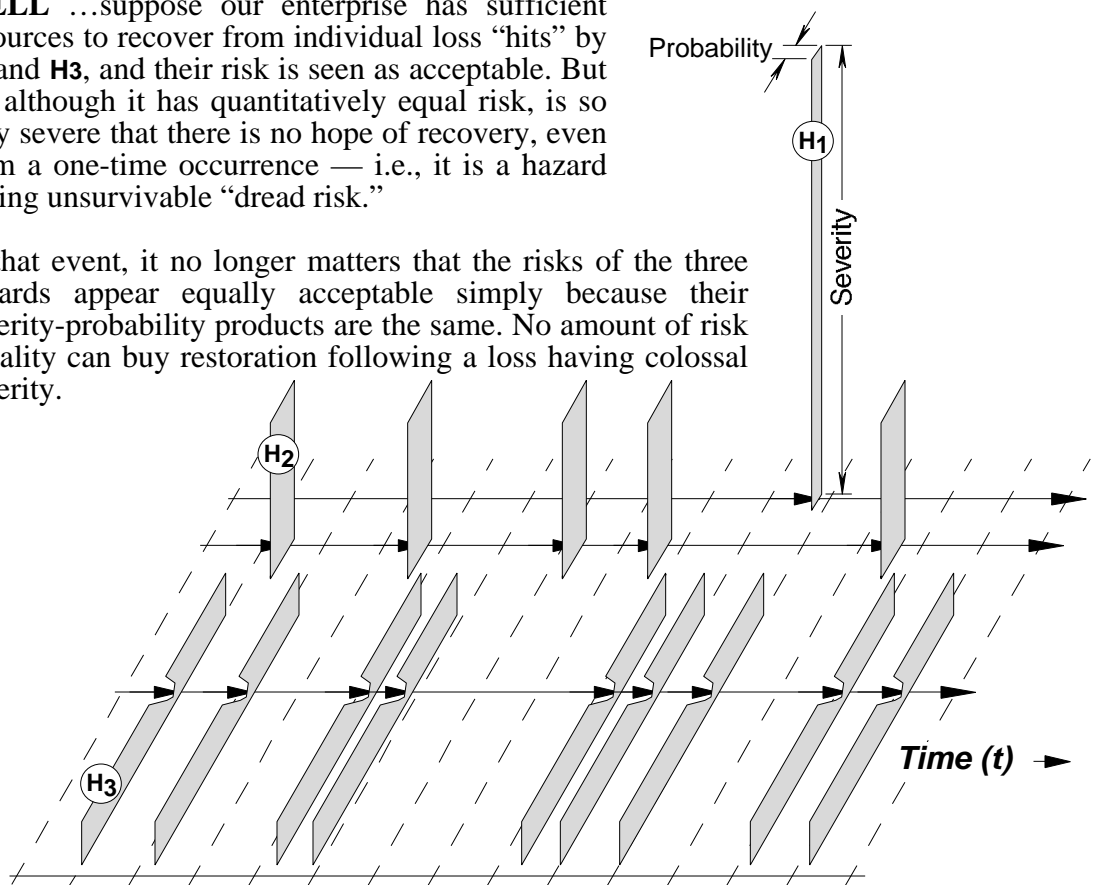
## — Are Equal Risks *Really* Equal? Consider a Spooky Inequity —

*...severity times probability should govern risk acceptance...  
but only up to an important point!*

**CONSIDER THREE HAZARDS** — Hazard **H1** has very small probability (bar width, in the sketch), but severity is enormous (bar height). Hazard **H2** produces much less severe loss events, but at appreciably higher probability of occurrence. Hazard **H3** produces frequent loss events, but at a very low severity level. So... the product of severity and probability for each of the three hazards can have the same value. That means *risk* is equal for the three. Shouldn't those equal risks mean that each hazard is equally acceptable (or unacceptable)?

**WELL** ...suppose our enterprise has sufficient resources to recover from individual loss "hits" by **H2** and **H3**, and their risk is seen as acceptable. But **H1**, although it has quantitatively equal risk, is so very severe that there is no hope of recovery, even from a one-time occurrence — i.e., it is a hazard posing unsurvivable "dread risk."

In that event, it no longer matters that the risks of the three hazards appear equally acceptable simply because their severity-probability products are the same. No amount of risk equality can buy restoration following a loss having colossal severity.



Notice, too, that because of its obvious high severity, **H1** may distract us from a need to deal with **H3**, which has equal risk. While we're concentrating on countermeasures against **H1**, our lunch will be eaten, bite-by-bite, by **H3**!

### *BOTTOM LINE*

If a hazard can wipe out the entire cosmos, it may no longer be so important that its risk appears to be acceptable simply because probability is very low. Hazards posing "acceptable" risk are acceptable only when recovery from an eventual "hit" is a real possibility!

# — Probability's Tough to Estimate? Consider the Means of Max and Min Values —

*...bounding can be easier than getting at a single value!*

**An Engineering Estimate of Failure Probability is Needed** for a system item, but you just don't feel comfortable coming up with a point value. Often in such cases you'll feel more confident at declaring maximum and minimum reasonable values for probability. So...why not simply make max and min estimates and take the arithmetic average?

You may be better off, as it happens, using the *logarithmic* average, i.e., the *geometric mean* ( $P_{GM}$ ) of max and min reasonable probability estimates. (See Box 1.)

And just *why* might this be better?  $P_{GM}$  differs from upper and lower bounds by *equal factors*. Consider an example: Suppose you reckon the maximum

**Box 1**

**PRINCIPLE:**  
Using Upper ( $P_U$ ) and Lower ( $P_L$ ) reasonable probability limits... }  $P_{GM} = \sqrt{P_U \times P_L}$

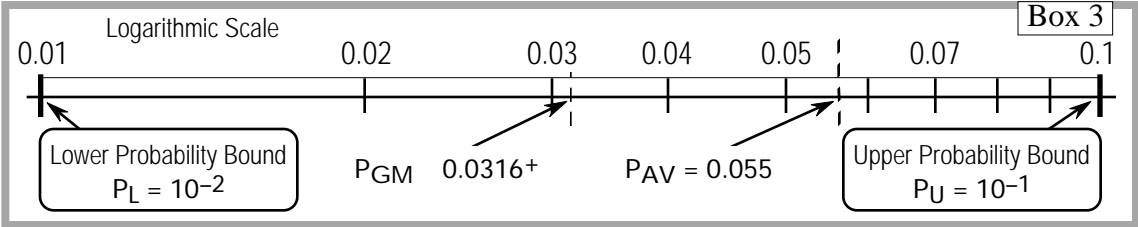
**Box 2**

**EXAMPLE:**  
For  $P_U = 10^{-1}$  and  $P_L = 10^{-2}$  }  $P_{GM} = \sqrt{10^{-1} \times 10^{-2}} = 0.0316^+$

reasonable value of the probability of interest to be  $10^{-1}$ , and the minimum reasonable value to be  $10^{-2}$ . The logarithmic average is now  $0.0316^+$  (Box 2). So, in this example, no matter where the true value of probability should actually fall within the range bounded by the max and min estimates, it can be no more than a factor of 3.16 from the  $P_{GM}$  value of  $0.0316^+$ .

That's because...  $\frac{P_U}{P_L} = \frac{P_U}{P_{GM}}$

The arithmetic average ( $P_{AV}$ ), however, would have been  $0.055$  ...more than five times the lower estimated bound and more than half the upper estimated bound (Box 3).



**BOTTOM LINE** —  
Before you try to get close to the middle of something by approaching it from its far edges, be sure you know what “middle” really means. Nothing will spoil your estimate like an off-center halfway point!

## — Reducing System Vulnerability... How d'ya lower a too-high $P_F$ ? —

*...here're hints for making your system a better survivor!*

- **Fortify Maintenance** — Increase the frequency of key maintenance activities; this will stretch MTBF.
- **Periodically Swap Out Parts** — Those that'll wear out because of the rise in their failure probability at the end of their random failure life. (See Scrapbook Sheet 02-8.)
- **Derate Components** — Design/select components that are notably more robust than needed to survive basic service stresses and environmental stresses.
- **Alter Architecture** — Make changes within the system structure, e.g....
  - **Add Redundancy** — Double up (or triple up, etc.) on critical system elements. (See Scrapbook Sheet 83-5, Example 1.)
  - **Relocate Existing Components** — Move items to more favorable indenture levels within the system. (See Scrapbook Sheet 83-5, Examples 1 and 2.)
  - **Loosen Coupling** — Make the system more “forgiving” by moving toward configurations in which there is less immediacy of internal component-to-component reliance.
- **Suppress Common Causes** — Identify common causes within cut sets and defeat them by isolating, shielding, insulating, etc. (See Scrapbook Sheets 86-4 and 87-4.)
- **Reduce Stresses** — This is the converse of derating components.
  - **Service Stresses** — Lower demands upon the system and/or items within it.
  - **Environmental Stresses** — Make the working environment less hostile.

---

*When selecting any vulnerability reducers, always consider...*

- Cost
  - Feasibility
  - Effectiveness
- } See Scrapbook Sheet 83-7

### *BOTTOM LINE*

There's more than one way to improve the long-term health of a system. Consider all of the options. The most obvious choice may not be the best one for your particular application!

## — When do you Revisit / Revise a Hazard Analysis and Risk Assessment? —

*...simply doing a good hazard analysis is only a good start.  
There are important times to RE-do the job, too!*

- **There's been a Near Miss (or, perish forbid, a Direct Hit)!** — A near miss can be an instance of nature whispering an important message to you about system vulnerability. Listen to the whisper and take advantage of it! Is the near miss scenario (or the loss event) explained by the hazard analysis for the system? Was a hazard overlooked, or a severity or probability level mis-declared? If so, revise the analysis.
- **The System has been changed** — Any change in system configuration or operating mode can introduce new hazards or alter declarations of risk for those previously recognized. Look for these differences any time the system is modified. Are there now new or altered components or subsystems? Don't ignore changes in operating procedures or levels of operator competence, and don't overlook changes in interfaces with other systems/subsystems or altered utility services. Make sure all of these things are considered in the analysis.
- **System Maintenance has been altered** — Changes in maintenance frequency or intensity can influence risk. Don't let maintenance protocol be changed without looking for the effects on hazards and their risks.
- **System Duty is different** — Is the system now going to be used for more severe duty (or, perhaps for more modest duty) than foreseen when the hazard analysis was last reviewed/revise? This, too, can introduce new hazards and vary risk for old ones.
- **Operating Environment is different** — Is the operating environment now to be different? This may have effects similar to those for system duty differences. (See above.) Consider temperature, humidity, barometric pressure, weather, vibration, radiation — all the stresses that may be associated with operating environment.

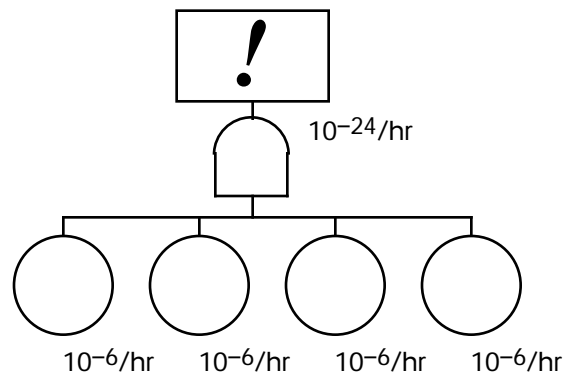
### *BOTTOM LINE*

A hazard analysis and risk assessment should be an "evergreen" document that changes as the system changes. An analysis that molds in a file drawer while the system undergoes alterations just isn't doing its job for the system proprietor!

## — Your Logic Tree Analysis Gives a Preposterously Low Failure Probability? —

*...you've probably failed to account for the HIGH stuff!*

- **AN ABSURDLY LOW  $P_F$**  is likely the result of a carelessly incomplete analysis using one of the logic tree methods — i.e., Fault Tree Analysis, Event Tree Analysis, Cause-Consequence Analysis, etc. Ridiculously low  $P_F$ s are to be distrusted. Why?
- **CONSIDER, FOR EXAMPLE,** our Mr. Zealous Designer who, fearful of system loss through failure of a component having a probability of primary failure of, say,  $10^{-6}/\text{hr}$ , seeks to suppress vulnerability by using four, like components arranged redundantly. The apparent failure probability is now  $10^{-24}/\text{hr}$ , the ludicrously low number shown here. That'll give a comfortably long apparent MTBF for even the most assiduous designer/analyst — around about  $1.14 \times 10^{20}$  years.\* Seem outrageous? You bet — it's downright preposterous!



- **SO, THEN — WHATEVER CAN IT MEAN** when an analysis produces such a teensie little number? What it truly means is that something that *hasn't* been analyzed will produce the analyzed loss event with much more probability than what *has* been analyzed. For example, the analysis has failed to take into account the influence of common cause effects (Scrapbook Sheets 86-4 and 87-4), or it does not recognize command faults (Scrapbook Sheet 86-12). Those common causes and those command faults have now become the sources of peril for the system. Unless they are accounted for in the analysis, the analyst has been deluded into thinking he's achieved a glorious victory over vulnerability with his little bitty number!

\* **Nifty Order-of-Magnitude Shortcut Clue:** To find MTBF for a known  $P_F$ , assuming a full-up, continuously operating, 'round-the-clock device and using the exponential distribution (Scrapbook Sheet 97-3), proceed as...

$$\text{MTBF [for } P_F = 10^{-n}/\text{hr]} \quad 1.14 \times 10^{(n-4)} \text{ yrs.}$$

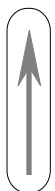
### *BOTTOM LINE*

Remember that the probability of our planet's annihilation by collision with an extraterrestrial object is about  $10^{-14}$  per hour (Scrapbook Sheet 87-3). If your analysis results in a  $P_F$  that's much lower than  $10^{-14}$  per hour, it's quite possible you've neglected extraterrestrial hits.

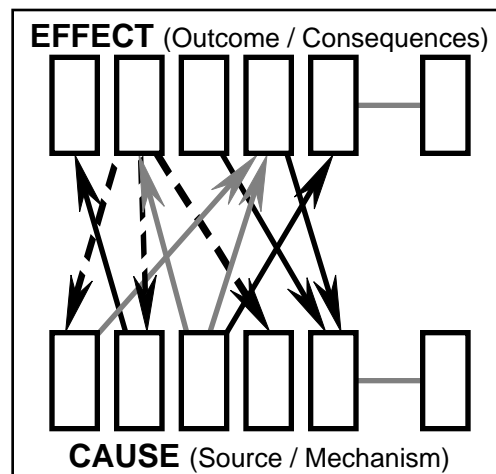
— Some Analyses Move *Bottom-up*,  
Some Move *Top-down*,  
and Some Move *Both Ways!*—  
*...make sure you are moving in the same direction as your analysis!*

- **BOTTOM-UP, or TOP-DOWN? ...and DOES IT EVEN MATTER?** — Some analytical techniques move in one direction, some in the other, and at least one goes both ways. Knowing which direction you're moving in improves your view of the strengths and limitations of the method you're using. Let's take a look...

- **FAILURE MODES AND EFFECTS ANALYSIS** Here, the analyst selects an indenture level within the system and moves through it with regimental rigor, posing these two classical queries for each item encountered: (1) *how* can this item fail (the failure *modes*), and (2) what are the harmful *results* (the *effects*) of each of these modes of failure. *[Bottom-up]*



- **FAULT TREE ANALYSIS** The analyst postulates a particular loss event, then explores in reverse, inquiring what elements of cause within his conceptual model of the system are capable — either singly or in combination — of bringing about this loss outcome. *[Top-down]*



- **PRELIMINARY HAZARD ANALYSIS** The analysis can begin either by recognizing potential causes of harm within the system or with foresight as to undesirable loss outcomes. From either of these, the analysis moves toward the other, constructing a hazard description as a miniature scenario that expresses the *Source*, the *Mechanism*, and the *Outcome* of the loss event to characterize each hazard. *[Bi-directional]*



**BOTTOM LINE**

When doing an analysis, it pays to ponder where you're starting from and which way you're heading. It'll help you to recognize real important stuff — for example, how to know when you've *arrived* somewhere!

— *BUT ...YOU GOTTA KNOW YOUR SYSTEM! ...OR NOTHING WILL WORK!* —

# — Using a Hazard Inventory Technique? How Do You Know Total System Risk? —

*...watch out — the line-item methods conceal Total Risk from view!*

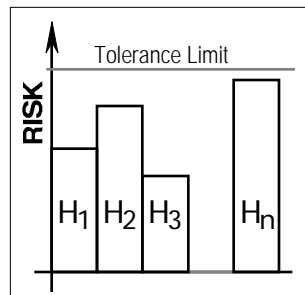
- **THOSE HAZARD INVENTORY TECHNIQUES**, Preliminary Hazard Analysis, Failure Modes and Effects Analysis, and their many derivative methods — they all

HAZARDS*	SEVERITY**	PROBABILITY**	RISK**
H <sub>1</sub>	S <sub>1</sub>	P <sub>1</sub>	R <sub>1</sub>
H <sub>2</sub>	S <sub>2</sub>	P <sub>2</sub>	R <sub>2</sub>
H <sub>3</sub>	S <sub>3</sub>	P <sub>3</sub>	R <sub>3</sub>
H <sub>n</sub>	S <sub>n</sub>	P <sub>n</sub>	R <sub>n</sub>

(\*From PHA, FMEA, etc.) (\*\*From Risk Assessment Matrix, e.g.)

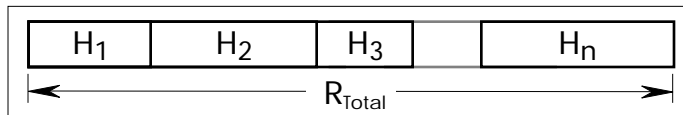
produce line-item listings of individual hazards (i.e., threats of harm). Subjective item-by-item assessments of risk are made in terms of severity and probability, hazard-by-hazard.

All of this is done at elemental levels within the overall hazard structure.



The view of overall system risk given by this approach is that of an inventory table. If risk for each of the individual, line-item hazards is acceptable, the analyst is led to believe that whole-system risk is also acceptable. A bar chart representation of the results makes this even more apparent.

- **SO, WHERE IS TOTAL SYSTEM RISK?** — It simply doesn't appear — not when the hazard inventory methods are used! Nature doesn't consult the inventory table in arriving at total system risk. Recognize that the individually tabulated hazards are *independent* — i.e., for the most part, none of them causes or is caused by any of the others. (That's just because we customarily express hazards that way.) Therefore,



the risks of the individual hazards actually *sum*. Those bars stack, end-to-end. But the hazard

inventory techniques never produce this grand sum. Instead, they conceal it, leading to the delusion that the system is “safe” on the argument that the individual hazards pose acceptable risk when viewed singly.

$$R_{Total} = \sum_{i=H_1}^{i=H_n} S_i \times P_i + S_2 \times P_2 + S_3 \times P_3 + \dots + S_i \times P_i$$

### BOTTOM LINE

It matters not at all that each individual mosquito within a large swarm may be an acceptable nuisance. Ask the fellow who's been swarmed by a zillion individually “safe” bugs how he got all those ugly, itchy welts!

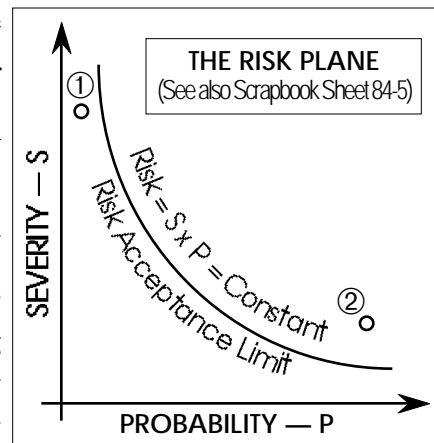


— *Always* Assess Risk for “Worst-Credible Outcome”  
 ...that’s a *Great* Convention,  
 except when it doesn’t work! —

...“worst-credible” can be “most-misleading!”

- **Worst-Credible Outcome** — It’s the often-used convention of practice in risk assessment: *assess risk for the worst-credible outcome*, meaning of course, for the worst credible *severity* of outcome for a given hazard. And that convention usually works quite advantageously. (See Scrapbook Sheet 84-5.) It certainly conserves resources by directing our analytical efforts away from trivial cases and toward the heavy-hitters.

- **Consider an Exception** — Let’s look at a hazard that has two, mutually exclusive outcomes. That is, the hazard scenario ends with either Outcome ①, or Outcome ② — never with any other outcome, and never with both. Outcome ① has very high severity, but probability is so low that risk falls comfortably below the threshold of tolerance. Outcome ② has much lower severity. So...we’ll ignore it following our “worst-credible” rule, even though its probability is quite high. Notice, though, that risk for this low severity case — the one we just ignored — is actually much greater than risk for the high severity case. In fact, as sketched here, risk for the low severity outcome can fall well above the acceptance limit.



- **How to avoid this?** — One good way is to construct each hazard description around a miniature scenario that expresses three important features of any hazard: Source, Mechanism, Outcome. (This is always a good practice, in any case — see Scrapbook Sheet 98-1) So if there are *two* or more outcomes, there are *two* or more hazards, not one! And risk for each is assessed separately.

*BOTTOM LINE*

So, we’ve got this teething puppy, and we’ve hidden those priceless heirloom sofa cushions in the attic until it’s over. That gives “worst credible” a pretty low probability, but let’s remember we’ve still got a whole houseful of much less expensive chewables in high-probability peril!

## — Describing Hazards?

Think *Source / Mechanism / Outcome* —  
*...a disaster is not a hazard, although it may be the result of one!*

*Finding* hazards is one thing (see Scrapbook Sheet 87-2), *Describing* hazards is another! Too often, our hazard descriptions don't describe *hazards* — instead, they name hazard *outcomes*. Some examples:

“Head-on collision”

“High-frequency hearing loss”

“Toxic spill”

Each of these outcomes is a result of other things that, taken together, do constitute a hazard. Examples: “Rain-slick pavement leading to skid and head-on collision with opposing traffic,” “Operation of vane-type compressor producing high sound pressure levels in occupied work area,” “Overpressure failure of UnFO<sub>3</sub> containment system.” Scrapbook Sheet 84-3 gives example “pseudo hazards.”

A hazard description contains three elements that express a threat:

- **a source** — an activity and/or a condition that serves as the root.
- **a mechanism** — a means by which the *source* can bring about the harm.
- **an outcome** — the harm itself that might be suffered.

These three elements, *source*, *mechanism*, and *outcome*, express what is often called a *hazard scenario* — a brief narrative description of a potential mishap attributable to the hazard. This brief scenario expresses a *threat of harm*. It is the *hazard description*. (For a *hazard definition*, see Scrapbook Sheet 98-2.)

An open-topped container of naphtha may be a source, but without a mechanism and an outcome, is it a hazard? Suppose it's in the middle of a desert — no ignition sources and no personnel within several miles? Not much of a hazard. Relocate it to the basement of an occupied pre-school facility near a gas-fired furnace. Source, mechanism and outcome now become clear — and it's a hazard.

A hazard description need not *specifically* address each of these three aspects — some of them may be implied and obvious. And it need not express them in a particular sequence. However, it should be possible to infer all three of them from the

### BOTTOM LINE —

Inert gas is not a hazard, but it may be a *source*. Asphyxia is not a hazard, but it may be an *outcome*. A leak is not a hazard, but it may be a *mechanism*. So ...here's a hazard description:

- Inert gas [*source*]
- leaking to displace oxygen from an occupied confined space [*mechanism*],
- resulting in asphyxia [*outcome*].

— Use a *HAZARD DEFINITION*  
that's not too *HAZARDOUS*—

...the way we define "HAZARD" affects what  
we find as hazards — and we want to find them all!

Need a good working definition for the term "hazard?" Proceed with caution! Far too many definitions have appeared in the literature of the field. Be especially wary of lengthy definitions and those that insist that a thing qualifies as a real hazard only if it involves the flow of energy in ways as to cause harm. Here's an example — a nice long definition from a popular textbook. Notice it's insistence on the necessity of a link to the release of energy:

Uh, oh!➔

**"Hazard:** A condition or situation that exists within the working environment capable of causing an unwanted release of energy resulting in physical harm, injury, and/or damage."

This thing's got the flow of *real literature* to it! It presumes little more than that the user will recognize the important distinctions between a "situation" and a "condition," and how "harm" differs from "damage."

Let's now suppose that we come upon an occupied, unventilated confined space in which the occupants, through ordinary respiration and basic metabolic processes, can deplete the oxygen concentration to a level below that which is necessary to sustain life. A real hazard? ...sure 'nuff! Does this definition *see* it as a hazard? ...nope! — no "unwanted release of energy," hence no hazard. This definition would also need awkward interpretation to recognize a lot of other obvious nastiness as real hazards — for example, negative stability margin of an experimental aircraft, or runaway recombinant DNA unloosed from a microbiology lab.

Here's a somewhat shorter and far less eloquent definition:

Better➔

**"Hazard:** A threat of harm."

At its simplest, a *hazard* is a just threat of harm to a resource having value — for example, a menace threatening personnel, or equipment, or the environment, or productivity, or the product of an enterprise. (See, also, Scrapbook Sheet 84-3.)

Using this definition, is that occupied, unventilated confined space a hazard? Yep! ...also that airplane that flies best backwards, and even that revolt of the genomes.

*BOTTOM LINE*

When defining the fundamental concepts of the trade, strive for brevity and simplicity. The term "hazard" is a good example. There's not another term used in the practice of System Safety that's more fundamental or more important — *or any less well understood.*

## — Too Many Methods?

### try *TYPES* and *TECHNIQUES*—

*...classifying the tools can make them easier to use outta the tool box!*

- **ONE of the PROBLEMS with SYSTEM SAFETY** is its stupefying proliferation of analytical approaches. The the 2<sup>nd</sup> Edition of the System Safety Society's *System Safety Analysis Handbook* describes 101 of them. To keep them all in their places in the toolbox, try a taxonomy that'll break them first into those that are...

(1) **Types** of analysis that address *what* is analyzed or *where* within the system or *when* the analysis is carried out, and those that are

(2) **Techniques** of analysis, addressing *how* the analysis is performed.

#### **ANALYTICAL TYPES**

The *WHERE, WHAT, WHEN* of Analysis

##### **EXAMPLES:**

- Preliminary Hazard Analysis (when)
- Subsystem Hazard Analysis (where)
- Software Hazard Analysis (what)
- Occupational Health Hazard Assessment (what)
- ...many others

#### **ANALYTICAL TECHNIQUES**

The *HOW* of Analysis

##### **EXAMPLES:**

- Preliminary Hazard Analysis (how)
- Failure Modes and Effects Analysis (how)
- Fault Tree Analysis (how)
- Probabilistic Risk Assessment (how)
- ...many others

Notice that Preliminary Hazard Analysis is both a Type (ideally, it's begun first) *and* a Technique (it's a hazard inventorying method). Notice also that it's possible to use Failure Modes and Effects Analysis (*how*) to perform a Subsystem Hazard Analysis (*where*).

The Techniques can be further divided into those that are **Top-Down** and those that are **Bottom-Up** (see Scrapbook Sheet 97-9), and further still into those that are **Hazard Inventory** methods (like Failure Modes and Effects Analysis) and those that are **Logic Tree Methods** (like Fault Tree Analysis).

As yet another useful distinction, some Techniques analyze **Forward** either chronologically or in a stepwise sequence of system states, and some move **Backward**. Event Tree Analysis, for example, always moves forward. Fault Tree Analysis can move backward.

#### **BOTTOM LINE**

*Be not boggled by this:* an **Event Tree Analysis** is a **Technique** rather than a **Type**, it's **Bottom-Up** rather than **Top-Down**, it's **Forward** rather than **Backward**, and it can be used to perform a **Subsystem Hazard Analysis!**

Know your tools, and both what they *will* do and what they *won't*.  
*You cannot win a tennis match with a bumper jack!*

## — Assessing Risk for a *Human* Target? Use either a *Long Exposure Interval...* or a very *Gullible Human!*—

*...people are important — assess their risks as though we mean it!*

- **THE EFFECT OF EXPOSURE INTERVAL** on risk is obvious. (See Scrapbook Sheet 84-4.) Risk for a given hazard-target combination can be expressed as the simple product of Risk's Severity and Probability components, and the Probability component is a function of the *Exposure Interval* — that is, the operating duration — whether expressed in manhours, or miles driven, or yards of fabric produced, or missions flown, or... So, a longer interval of exposure to a particular hazard means higher Probability, which means greater Risk.
- **WHEN PEOPLE ARE HAZARD TARGETS** a special precaution is called for in picking the exposure interval. If the severity component of risk is high but the activity is to be brief, it becomes tempting to use that brief activity period itself as the exposure interval. Why not? If you're only gonna have Clarence do this nasty job *one brief time*, why assess risk for more than the 8-hour exposure it'll take him to finish? Well, there's a *good reason!* It's because you're going to want Clarence around long enough to do *many* jobs. Many of them may be equally brief — and may pose equal severity.
- **HERE'S A SCENARIO** that shows why it's important to use a **LONG EXPOSURE INTERVAL** when assessing Risk for hazards to personnel, even though job-by-job Severity and Probability can make risk appear benign. The risk analyst for today's job lacks control over future job assignments. Lifetime Risk burden can accumulate to an overwhelming level if job-by-job risk assessments are based on the brief durations of successive jobs, some of which may have high Severity components of risk.

A trusting worker is told that his job assignment for the day is to aim a revolver at his head, spin the cylinder, then squeeze the trigger, *just once!* He is assured that the risk for this operation has been competently assessed and, even though the severity component is catastrophically fatal, risk is acceptable. The revolver's cylinder has 10,000 chambers. Only one chamber contains a live round. All others are empty. The probability component of risk for that one-day assignment is then a very low  $10^{-4}$ . The worker accepts the assignment, survives, and reports for work the following day, when he's told the same thing. Again, he accepts. If risk was acceptable for this job yesterday, why not today? Over a 40-year working lifetime at this assignment — i.e., about 10,000 workdays — the worker's probability of succumbing to this hazard will have become greater than 60%. *Seems grim!* Shouldn't we give him better odds of being around for a full working lifetime?

### **BOTTOM LINE**

When assessing risk for a short-term hazard to a long-term human, decide first whether you'd like the *human* or the *hazard* to survive! Use the *human's working lifetime* as the probability interval unless you have greater concern that the *hazard* should endure!

## — Need a *RISK ASSESSMENT MATRIX*? Here's a “*Starter Kit*” —

*...numerical methods are for people who've got numbers,  
matrices are for the numerically deprived!*

- **RISK ASSESSMENT MATRICES ABOUND**, and everybody's got at least one. There's no “magic” to the matrix. It's just a tool — an important one — that gives access to experience-based judgment as a substitute for quantitative calculations. That's mighty useful when you don't have the quantities to calculate or the resources to do it. It's a tool that can be used with all of the hazard-inventory analytical methods — e.g., Preliminary Hazard Analysis.

Add and scale other targets as needed — e.g., the Environment, the Product, Productivity (Down Time), Proprietary Information — management decides which ones apply.

**Mishap Probability** \*30-yr Exposure Interval

So unlikely it can be assumed occurrence may not be experienced\*  
Physically impossible to occur\*  
Not likely to occur, but possible\*  
Likely to occur sometime\*  
Likely to occur several times\*  
Likely to occur repeatedly\*  
Likely to occur frequently\*

IMPOSSIBLE    F\*    IMPROBABLE    E\*    REMOTE    D\*    OCCASIONAL    C\*    PROBABLE    B\*    FREQUENT    A\*

The Matrix should be “tailored” for the enterprise at hand. Adjust risk tolerance boundaries and scaling of axes to suit management / proprietor needs.

Mishap Severity												
PERSONNEL	EQUIPMENT											
Death	> \$1M	<b>I</b> CATASTROPHIC										
Severe injury or severe occupational illness	\$250K to \$1M	<b>II</b> CRITICAL						②	①			
Minor injury or minor occupational illness	\$1K to \$250K	<b>III</b> MARGINAL			③							
Less than minor injury or illness	< \$1K	<b>IV</b> NEGLIGIBLE										

**Risk Code Actions**

③

Operation permissible.

②

Operation requires written, time-limited waiver, endorsed by management.

①

Imperative to suppress risk to lower level.

Adapted from MIL-STD-882D

### • A FEW “WATCH-OUTS”

- Pick the Exposure Interval with care! See Scrapbook Sheets 84-4 and 99-2.
- Include an **F**/Impossible probability level to score zeroed post-countermeasure risk.
- Try some sample hazards on a new matrix before unleashing it on the entire cosmos.

**BOTTOM LINE**

The matrix *won't* help you *find* hazards. You have to do that. Then it'll help you assess their risks. But it'll *never* make you “safe.” Nothing will! There is no absolute safety! A thing — anything — is safe only to the degree that we are willing to accept its risk!

## — Risk Matrix Interpretation Troubles? ...try “Calibrating” for Clarity — *...for a better fix on guesswork, begin with something that’s known!*

- **AN OFTEN PERPLEXING PROBLEM** in using the Risk Assessment Matrix, especially for the novice, lies in finding a sense of “feel” for the degree of risk represented by the various matrix cells. Even a seasoned group of analysts can find opportunities for exciting debate on issues of interpreting which cell properly represents risk for a specific hazard. Developing a hazard scenario that can be attached with confidence to just *one* matrix cell can make interpreting the whole matrix a lot easier.

A persuasive cell to use as such a “calibrator” is one at the highest level of severity, **I/Catastrophic**. At that level, find a hazard scenario that satisfies these two criteria:

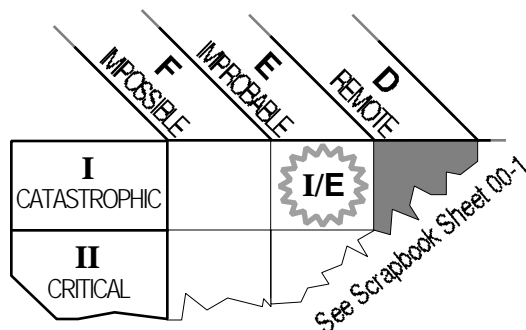
- 1) It has risk that’s now accepted, but for which countermeasures would surely be invoked were its catastrophic outcome to be suffered with any greater probability.
- 2) It is familiar to the community of analysts who’ll be using the matrix — something they’ve all “seen.”

There *is* just *one* matrix cell that satisfies the first criterion — it’s **I/E**.

Here’s a hazard ensemble used at one work location to satisfy the second criterion:

**Cell I/E =**

Risk from the ensemble of hazards that accompany commuting by private auto, over a working lifetime of exposure (i.e., 25-30 yrs), over a heavily trafficked, two-lane, 15-mile codeworthy highway passing through mixed rural-urban areas, with occasional chuckholes, crossing wildlife, hydroplaning, etc. as threats.



Severity for this hazard ensemble is clearly **I/Catastrophic** — it has killed people. As to the *probability*, it’s certainly not **F/Impossible**, and neither is it as high as **D/Remote**, where additional countermeasures to reduce risk would unquestionably be mandated — i.e., risk at Cell **I/E** is *accepted*, but it would not be if matters were any worse. *Only* the **I/E** cell expresses this

- **THE PRINCIPLE** at work here is a simple one: Even at the very highest level of severity to be found in the matrix — i.e., **I**, there must be a small but finite probability for which risk is acceptable, else we would not drive to work. That probability is **E**.

**BOTTOM LINE**

When measuring using a ruler having unfamiliar dimensions, you’ll have a better appreciation for the result if you first use it to measure something else having familiar dimensions that you know with confidence.

— Vexed over Fault Tree  $P_{TOP}$  *ACCURACY*?  
 Maybe there's *NO NEED*...Here's Why! —  
*... $P_{TOP}$  can be a rascal to get your arms around...*  
*but, are you really sure you need to hug it all that tight?*

- **IN DOING A FAULT TREE ANALYSIS**, we too often seek to perfect our imagined grip on accuracy. It's the same mystical notion we succumb to when we say we need "four nines on reliability, with 95% confidence." Life is just not like that. (See Scrapbook Sheet 97-1.) With Fault Tree Analysis, we're most likely mixing a few actuarial input data with many engineering estimates, and we're doing very well to end up with a **TOP** probability that's within half an order of magnitude of "Golden Truth," which itself will have an exact value not known to any mortal among us. Here *are* a few *real* Golden Truths:

- **JUST WHY DID WE GROW THIS TREE ANYWAY?**

- Was it to discover whether  $P_{TOP}$  represents Risk that's acceptable? If all of the probability values entered in the analysis are made a skotch high, then  $P_{TOP}$  is biased pessimistically — i.e., it's a similar skotch high. And if Risk is acceptable at that pessimistic value of  $P_{TOP}$ , then there's no justification for either further worry about accuracy or further refinement of input data.
- Was it to compare two competing design alternatives? If trees for both are grown using similarly garnered values of input probability, then the absolute values of  $P_{TOP}$  are of much less importance than is the difference between them.

- **WON'T FURTHER GROWTH IMPROVE ACCURACY?**

- Not necessarily. The tree *level* at which we stop is of less importance than is the need to stop at a point where we feel reasonably confident of the accuracy of the input data, at whatever level that may occur. (See Scrapbook Sheet 86-5.)

*BOTTOM LINE*

If the speedometer is known to read high, and it shows that you're within the speed limit, you don't need a better speedometer to be sure that you're not speeding.



— Does *RISK* seem just a little too *HIGH*?  
...then try some *Chicanery to Lower It!*—  
*...it doesn't take much quackery to establish practice as a charlatan!*

**SYSTEM SAFETY** is a field in which fakery is easily practiced — and, unfortunately, it often goes undetected. Here's a short list of some of the field's favorite frauds for use when risk seems unacceptably high:

- **SHORTEN THE EXPOSURE INTERVAL** — If a 25-year exposure interval is making the probability component of risk too high, switch to 25 nanoseconds. *That'll drop apparent risk, right now!* Better yet, don't disclose the exposure interval you're using to anyone — especially to exposed personnel — and let it change from hazard to hazard and from target to target. If you're discovered, point out that you've striven to achieve analytical flexibility. (See Scrapbook Sheets 84-4 and 99-2.)
- **DROP THE INDENTURE LEVEL** — You've got a Fault Tree for an assembly that has no redundant counterparts, but it does contain redundant components within its own innards. The tree shows too much probability that the assembly'll fail owing to the threat of co-existing faults of those redundant components. Give up on the Fault Tree. It's the wrong method. Switch to a bottom-up, hazard inventory method (e.g., Failure Modes and Effects Analysis). Work it way down there at that redundant component level. This'll produce an impressive pile of paper, indicating wholesome thoroughness. It'll examine *every one* of those redundant components, and it'll show only *benign outcomes* for their individual failures. (If any one of them dies, it has redundant counterparts to take over its burden.) *And* this'll be an analysis that's just not smart enough to deal with the probability of those co-existing component failures that were causing you the grief in the first place.
- **IGNORE OPERATIONAL PHASING** — So, you've perceived nasty risk for some of those spooky mission phases like takeoff and landing. Ignore them. After all, they occupy just a really *small* part of the system's overall operating duration. Instead, concentrate on the system's hazards and assess their risks for the much lengthier (but benign) mission phase of cruising in level flight at 30,000 ft. in clear air with full fuel tanks and power levers set on "cruise" where nothing bad ever happens. (See Scrapbook Sheet 86-3.)

*BOTTOM LINE*

When an analysis shows a sick system, *do not succumb* to the temptation to "fix" the analysis rather than to cure the system. If you do, by and by, the client will find himself surrounded by trash. And you can count on him to catch on!

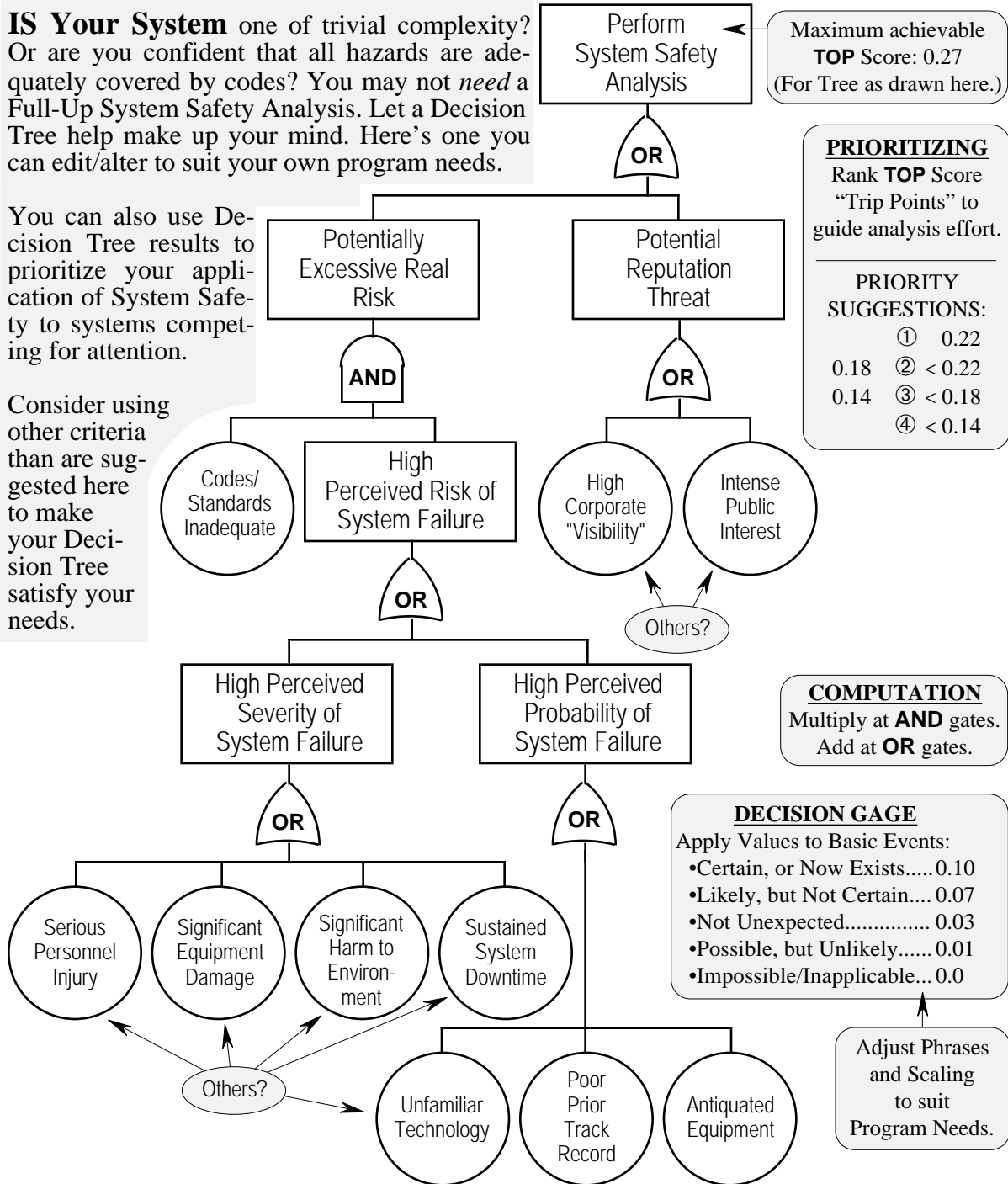
# — Maybe not *ALL* Systems deserve analysis ...how d'ya DECIDE?—

...here's a Starter Kit Decision Tree to put discipline in an arbitrary process!

**IS Your System** one of trivial complexity? Or are you confident that all hazards are adequately covered by codes? You may not need a Full-Up System Safety Analysis. Let a Decision Tree help make up your mind. Here's one you can edit/alter to suit your own program needs.

You can also use Decision Tree results to prioritize your application of System Safety to systems competing for attention.

Consider using other criteria than are suggested here to make your Decision Tree satisfy your needs.



**BOTTOM LINE**

Too often, we analyze because we know how to analyze rather than because analysis is necessary. Reserve the really tough analyses for the really deserving cases. System Safety should guide the prudent designer and should then amount to documenting the thoughts that the prudent designer should be thinking in developing the design, or the operating procedure, or the... and little more than that.

## — Economic Aspects of System Safety

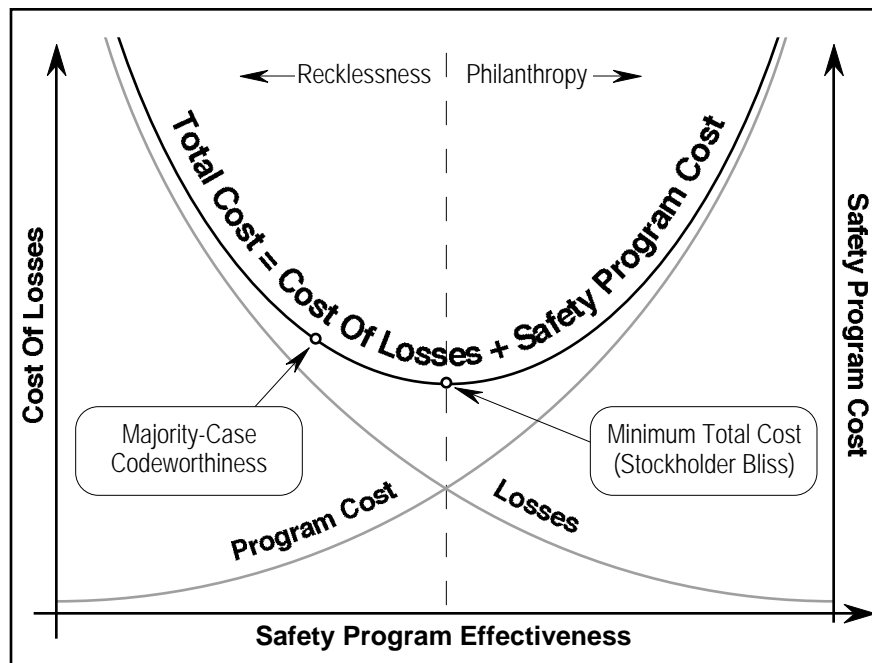
### *When is it worth practicing? —*

*...is there a balance between cost of losses and cost of "safety?"*

**TOTAL COST** of Safety Program successes and failures is divisible onto Program Operating Costs and Cost of Losses not foreseen / avoided. The System Proprietor bears the burden of this simple summation. If the *proprietor* doesn't add it up, then nature *does!*

<b>\$TOTAL =</b>	<p><b>Program Cost:</b></p> <ul style="list-style-type: none"> <li>• Program Development</li> <li>• Staff Operating Costs</li> <li>• Training</li> <li>• Enforcement</li> <li>• Inspections / Audits</li> <li>• Equipment</li> <li>• ...etc.</li> </ul>	+	<p><b>Losses:</b></p> <ul style="list-style-type: none"> <li>• Manhours</li> <li>• Workers Compensation</li> <li>• Schedule Delays</li> <li>• Productivity Sacrificed</li> <li>• Equipment Damage</li> <li>• Fines / Penalties</li> <li>• ...etc.</li> </ul>
------------------	---	---	--

To produce a more effective Safety Program, operating cost rises. This lowers the cost suffered in Losses. There exists a ponderable but elusive point at which the sum of these two factors is a minimum. For many systems, particularly those at the cutting edge of technology, codeworthiness alone is inadequate to balance the cost of the Safety Program against the cost of Losses. Applying the practice of System Safety in such cases further reduces losses to establish a true minimum total cost.



However, no matter how much resource outlay is devoted to support the Safety Program, the cost of losses can never be expected to fall to zero. It may be very small, but finite!

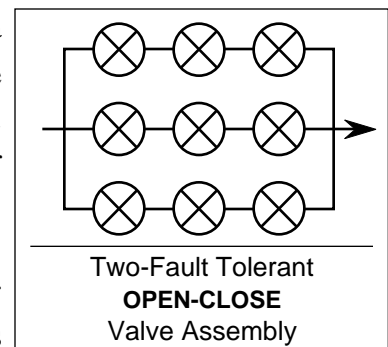
**BOTTOM LINE** —

In devoting added resources to preventing losses, eventually a point will be reached beyond which additional resources will earn less than their worth in loss reduction. To operate economically, stop at that point. *BUT*, if *people* are targets? ...well that's *another* matter!

— “Fault Tolerance”  
 ...only a *Sometimes* Answer to Reducing Risk —  
 ...but be sure you pick the right “sometimes!”

**SOME DESIGN CRITERIA** — instead of specifying allowable minimum *Reliability* or maximum *Failure Probability* — require that a system or a sub-element within a system must be capable of performing its critical function after suffering one, or two, or even three co-existing internal faults. *Nature, not the designer*, selects which internal elements to fault and in what mode(s). Such requirements can indeed be onerous!

**CONSIDER**, for example, the requirement that a particular, critical OPEN-CLOSE valving function must be two-fault tolerant. The result is an assembly of nine valves. Any two valves can fault, each of them either open or closed, and the OPEN-CLOSE function then remains intact.



For the configuration shown here, if failure probabilities for both OPEN and CLOSE functions for each of the nine valves

are equal at  $(P_{O-C}) = 10^{-2}$ , then overall failure probability for a single OPEN-CLOSE cycle of the nine-valve assembly is  $3.0 \times 10^{-5}$ . *Impressive!*

$$P_T = 30 \times (P_{O-C})^3$$

**BUT** — this design *does* have its *drawbacks!* For example, there are now *many* potential leak points. And if this thing's in a weight- or space-tight environment, it's likely to lead to selecting smallish, frail valves. Because nothing's been said in the performance specification about *Reliability*, this nine-valve assembly may actually have greater *Failure Probability* than a single, very robust, high-quality valve for the same job. Would that single valve be easier than the nine-valve family to purchase? ...to inspect? ...to maintain? ...to replace? And, is there now some Common Cause that'll knock out the whole fleet of Fault-Tolerant components? (See Scrapbook Sheet 86-4.)

Think all of these thoughts when making the important decision whether to specify Minimum Acceptable Reliability, on the one hand, or Two-Fault Tolerance, on the other.

**BOTTOM LINE** —

The potential for failure can be successfully *populated* into submission  
*only if*

the mortality rate for each individual in the population is *adequately low!*

*Don't get flim-flammed into a flotilla of flimsy flapdoodles if one husky part'll do a better job!*

— Is *Programmatic Risk* your concern?  
 The *System Safety* methods'll do the job! —  
*...basic principles stay that way, no matter where they're found!*

- **Managing Programmatic Risk**, sometimes called *Technology Risk*, amounts simply to identifying threats that are posed to the important attributes of an enterprise — attributes such as *Cost*, and *Schedule*, and *Performance*, and then evaluating those threats in terms of their combined severity and probability of inflicting harm upon the objectives of the enterprise. Regard the threats as *hazards*, and their combined severity and probability become *risk!* When the threats pose risk at an unacceptably high level, action must be taken to control them. Sounds like System Safety, *deja vu?* THAT'S WHAT IT IS! Think of those Cost-Schedule-Performance attributes as *targets* to be protected. Those same old PHA, FMEA, Fault Tree and other techniques we use in everyday System Safety practice now become equally applicable in the Programmatic Risk domain.
- **A Risk Assessment Matrix** (Scrapbook Sheet 00-1) can be outfitted to deal subjectively with threats to any programmatic (or other) targets you may choose. Here are example matrix severity scales for a program in which the enterprise is to design a system that'll satisfy a particular set of mission performance requirements. Design *Schedule*, design *Cost*, and final system *Performance* are the attributes of concern here:

Severity					
PERSONNEL	EQUIPMENT	SCHEDULE	COST	PERFORMANCE	
Death	> \$1M	> 6 wk overrun	> 20% overrun	Total mission unachievable	<b>I</b> CATASTROPHIC
Severe injury or severe occupational illness	\$250K to \$1M	3 to 6 wk overrun	10 to 20% overrun	Major mission achievement compromise	<b>II</b> CRITICAL
Minor injury or minor occupational illness	\$1K to \$250K	1 to 3 wk overrun	5 to 10% overrun	Mission performance degraded	<b>III</b> MARGINAL
Less than minor injury or illness	< \$1K	< 1 wk overrun	< 5% overrun	Minor mission performance compromise	<b>IV</b> NEGLIGIBLE

The Matrix should be "tailored" for the enterprise at hand. Adjust scaling of severity and probability axes and risk tolerance boundaries to suit system management / proprietor needs.

System Safety Targets

Programmatic Targets

**CAUTION:** Make sure that the descriptors for levels of Severity apply to the targets you intend. In the above example, Schedule and Cost may apply to the effort to produce the design, whereas Equipment and Performance may apply to the final, designed system.

**BOTTOM LINE**

There's no more mysticism or metaphysics in Programmatic Risk Management than in System Safety practice. Threats are still hazards. Resources to be protected are still targets. Risk is still that same old familiar probability-severity doublet.

*Don't let yourself get bamboozled into flim-flammery by charlatans who seek to overcomplicate the basic principles!*

## Let us now reflect upon *POPULATION*

Does it affect the  
*SEVERITY* or the *PROBABILITY*  
component of *Risk*?

...the answer is YES — it surely DOES exactly that!

- **OFTEN HEARD** is the view that increasing *population* elevates the *probability* component of the severity-probability doublet that we all call *risk*. This makes intuitive good sense, and it's often *true!* BUT *NOT ALWAYS!* Let's try a close look...
- **CONSIDER FIRST** an analysis of a fair maiden in a castle tower — one who is in peril from a roving standard model, fire-breathing, hazard dragon. An assessment of the threat to the maiden from the dragon will produce a *value* representing *risk* over the period of dragon-castle encounter.
 

RISK FOR A SINGLE HAZARD-TARGET COMBINATION IS FIXED AS THE SIMPLE *SEVERITY-PROBABILITY PRODUCT!*
- **NEXT CONSIDER AN ENTIRE PASSEL** of dragons threatening the maiden in her castle under those same conditions. Or, consider a whole fleet of castle towers each inhabited by a maiden and exposed to that original dragon. The *PROBABILITY* that a maiden somewhere in that fleet of dragon-threatened castles will succumb to a dragon event is notably greater than is the probability for a population of just the one maiden in the single castle. This is the way population is intuitively viewed as affecting risk — i.e., by raising *PROBABILITY*.
 

INCREASING POPULATION OF *HAZARDS* AND/OR OF *TARGETS* INCREASES LOSS EVENT *PROBABILITY!*
- **BUT NOW CONSIDER** that original, single castle and that one dragon, but with *three times as many fair maidens* in the tower. A new risk assessment will show that *probability* of a loss event from the original dragon hazard has changed very little. Potential *SEVERITY*, however, will have been increased by the now-greater population of maidens\* who are vulnerable to that hazardous dragon.
 

INCREASING POPULATION OF *WORTHWITHIN* A TARGET INCREASES LOSS EVENT *SEVERITY!*

\***WATCH OUT!** For many risk assessment matrices, including the one found in MIL-STD-882D, the severity component of risk from exposure of a *multitude of people* to a particular hazard is seen as no different than risk for exposure of a *single person* to that same hazard!

### *BOTTOM LINE*

If you're insuring boats and passengers, it's important to count *how many* of each there are, AND *how many* icebergs'll threaten the trip. Probability increases with the number of icebergs and the number of boats. Severity goes up as we put more passengers on a boat.

## — Whadd'ya *EXCLUDE* from a Preliminary Hazard Analysis? —

*...available schedule and resources'll never let you include everything!*

• **DECIDING WHAT TO OMIT** from a System Safety study when using one of the hazard inventory techniques (e.g., Preliminary Hazard Analysis and its derivatives) is an important part of “scoping.” (See Scrapbook Sheet 96-1.) What do you rule *in*-bounds and *out*-of-bounds? Examine *everything*, and you'll never finish. Include too little, and you'll miss some of the important stuff. Like many things in System Safety, the decision rests more on art than science. Here are some candidate things to consider for omission, and statements that can be tailored to describe them; be sure those that're used appear in a formal descriptive statement of the Scope of the Analysis:

- Static system elements (i.e., without moving parts) in non-hostile environments. [e.g., load tested, codeworthy guard rails on indoor observation platforms.]
- System elements having MTBFs confidently known to exceed anticipated service life by very large margins. [E.g., in-conduit illumination wiring ...but *watch out!* Even an exposure interval as brief as  $10^{-3}$  MTBFs gives a *failure probability* as high as  $10^{-3}$ ; see Scrapbook Sheet 97-3.] [See item below for alternate wording.]
- Derated elements — i.e., those for which there is confidence that service stresses and environmental stresses will fall well within design ratings. [See item above.]
- Robust (i.e., de-rated/overdesigned) elements having few or no moving parts and not exposed to cyclic loading.
- Commercial, off-the-shelf elements having known-to-be-trustworthy performance histories.
- Non-critical human operator functions.
- Deliberate acts of sabotage.

See also Scrapbook Sheets  
96-1 (Scoping),  
01-4 (Analytical Assumptions), and  
01-6 (Limitations).

Done prudently, scoping helps focus the analytical effort for best payoff at evaluating system risk and at guiding methods to control it — but when in doubt, don't leave it out!

### *BOTTOM LINE*

The artist who's never sure when he's finished the painting/symphony/sculpture/essay would do well to declare, early on, just where the finish line lies, so's he'll know when he's reached it.  
*There's a lot of art in System Safety!*

— Don't assume the owner won't  
abuse the system ...*not without saying so!*—

*...to keep yourself honest and the proprietor informed, list the limits!*

- **THOSE ANALYTICAL ASSUMPTIONS!** ...when you make them, it's important to *say what they are!* Clearly you can't analyze *everything* for *every* eventual mischance that might befall the system. That's why you "scoped" the analysis to confine its size to manageable bounds. (See Scrapbook Sheets 96-1 and 01-3 for scoping and its importance.) But you also had to make certain assumptions regarding the degree of care to be taken by the system proprietor in operating and maintaining the system. *Those* assumptions are important *too*, and they should be set down for the proprietor to understand. (They can appear in your analysis plan and in the cover report that accompanies your final analysis.) Here's some starter kit language that lists a few of the assumptions that you might consider:

- Equipment will not be exposed to service stresses or environmental stresses exceeding design intent.
- Safe operating procedures for critical operations have been / will be prepared, reviewed for adequacy, and implemented by the system proprietor. ("Critical" operations are taken as those for which unmitigated risk falls at levels deemed unacceptable.) [See alternate, below.]
- Critical operations will be carried out by appropriately trained, tested, and certified personnel.
- Prudent standards of operating discipline will be implemented and maintained.
- Prudent standards of equipment/system maintenance will be imposed and practiced.
- Operations will be free from acts of deliberate mischief/sabotage.

...and then, as the analysis progresses, you may find that you'll want to return to your list of assumptions and edit it, dropping some and perhaps adding others. **DO IT!** Then make sure that *all* of the analysis conforms to the newly adjusted list!

**BOTTOM LINE** —

System Safety analysis is unlike grocery shopping. It's as important to *list* the things you *won't* buy as it is to enumerate the items you intend to purchase. You'll *never* analyze *everything*, just as you can't eat the entire contents of the store!



## — A Safety Report to a CLIENT? up-front *thinking* avoids later *grief!*—

*...useful service and lethal honesty must not clash!*

### SOME PRECAUTIONS TO OBSERVE IN SAFETY REPORTS

- **DO NOT deliver a First-Report “Surprise”...**

Prior to delivery of a report of analysis and findings, provide the client a complete draft, clearly marked (each page): “**PRELIMINARY UNCHECKED DRAFT.**” This will allow the client an opportunity to identify inadvertent use of expressions that might unintentionally place client resources in jeopardy.

**DO NOT compromise the tenets of ethical practice...**

Do not succumb to client pressure to develop/report findings that are contrary to regulatory or statutory requirements or that violate standards of sound professional practice.

**Tell the TRUTH ...(*absolutely*)**

If the client’s design of a system poses great risk, or if the Laboratory Eyewash Fountain doesn’t work, or if a code is violated, *say so!* ...but remember that it’s *the client* who decides how much risk he’ll take. (The System Safety practitioner evaluates the *amount* of risk, but it’s the system proprietor who decides whether to take it on.)

**Adopt an Insular Editorial Persona... (*i.e., advise without advising*)**

*Make no direct recommendations. Avoid use of such phrases as:*

“We recommend...”

“It is recommended...”

“We advise...”

“Following are our recommendations...” ...etc.

*Instead, use phrases that provide generous latitude of action for the client, e.g.:*

“Consideration should be given to...”

“Following are options of choice that bear consideration...”

“Alternative designs to be considered would include ...[list them]; still others may be developed and considered for adoption...”

**Think about the future!**

Ask yourself “How will this go down during the deposition?” (...or from the witness stand, etc.), and “Do I need this client more than I need my reputation?”

**When in doubt, seek counsel...**

*In any questionable case, seek the advice of Legal Counsel!*

**BOTTOM LINE**

The system owner knows things about his system and its intended use in ways you’ll never see.

Your job is to discover how much risk he’s got.

His is to decide whether the potential for gain outweighs the risk.

## Do you need a DISCLAIMER? *YES!* is the only acceptable answer!

You won't have delivered the moon, so let it be known!  
...keep both the *system* and the *analyst* out of hot water!

- **EVEN THE BEST SYSTEM SAFETY ANALYSIS**, at *some* point — and usually at *many* points — rests on *art* rather than *science!* Thus, there can never be absolute assurance of its accuracy or thoroughness. Perfection is unachievable. Don't let the recipient of the work think otherwise. Protect him and yourself from misunderstanding by disclaiming perfection. Do it in writing, as a part of your System Safety analysis report. Here are examples of a disclaimer and a limitations statement that can be considered for adaptation to your purposes. Involve your legal counsel in doing the adapting.

### DISCLAIMER

Within the scope of the work reported here, we warrant that we have exercised our best professional effort at analyzing hazards, assessing risk, and formulating conclusions as reported herein. However, we specifically disclaim any warranty, expressed or implied, that hazards will be completely eliminated or mishaps will be completely avoided or that any particular standard or criterion of hazard or mishap elimination will be achieved if the information presented here is taken as guidance. We do not accept liability for any loss, damage, or injury resulting from the use of this information.

### LIMITATIONS

Hazard analyses and risk assessments reported here have encompassed all aspects of system design which are unique to the client's purpose as expressed in the provisions of the Contract. They have not encompassed elements of system design which are found within items of routine manufacture, and which are intended to experience combined service stresses and environmental stresses falling demonstrably within component design ratings, and for which there is acceptable confidence of adequately controlled risk, based on prior experience. Hazards have not been considered which are routinely well mitigated by conformance to unequivocal codes, standards, and regulations.

### *BOTTOM LINE*

A disclaimer is *not* an allusion to chicanery but a *declaration of honesty!*

You cannot practice *perfection* and *art* at the same time.

*SAY SO!*

— *Probability Estimating, made easy!*  
 ...well, maybe just a *little bit easier*, anyway —

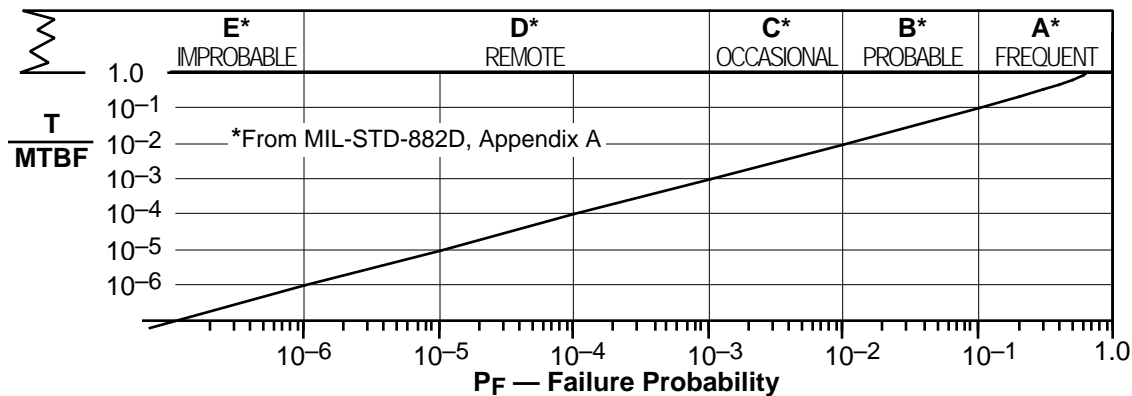
...when you can't estimate *how likely*, try estimating *how long!*

- **A SINGLE, QUANTITATIVELY EXPRESSED POINT VALUE** for random failure probability for an item within a system, or for the system itself, can be pretty hard to estimate. Sometimes it's easier to estimate reasonable upper and lower bounds, and then proceed as in Scrapbook Sheet 97-5. But even that can be daunting.

Often, the *operating duration* to be expected *between* random failures is easier to estimate than the probability of failure. Ask, "...in a large fleet of these things, just like this one in its present state, how long would an average one operate without failing?" Here, "how long" is the number of operating hours, or missions flown, or donuts stamped, or miles traveled, etc. Express this Mean Time Between Failures (MTBF) in the same units of measure you want for the exposure interval (T) for which failure probability is desired. The exponential model gives a straightforward relationship between MTBF and random failure probability (P<sub>F</sub>):

$$P_F = 1 - e^{-T} \left\{ \begin{array}{l} \text{where: } T = \text{exposure interval} \\ \quad = 1/\text{MTBF} \\ \quad = \text{Napierian base (2.718...)} \end{array} \right\} \quad \left. \begin{array}{l} \text{See Scrapbook} \\ \text{Sheets 95-3} \\ \text{and 97-3} \end{array} \right\}$$

From this relationship, here's a plot of the ratio of intended exposure interval (T) to Mean Time Between Failures (MTBF) as a function of Failure Probability (P<sub>F</sub>). Subjective probability expressions, A-E, corresponding to the numerical values, as found in MIL-STD-882D, are also shown.



Notice that for values of exposure duration (T) less than one tenth of the Mean Time Between Failures, there's no perceptible difference between failure probability (P<sub>F</sub>) and the ratio of exposure duration T to MTBF.

- **EXAMPLE:** We've got no P<sub>F</sub> data for our Mk-I Thrustplucker™, but we'd estimate that in a large bunch of them, each will randomly poop out, on average, every 27 months of continuous 24-hr service ( 20,000 hrs). Ours'll run a 500-hr. duty cycle. Its estimated failure probability over that interval is then 500/20,000, or 2.5 x 10<sup>-2</sup>. This amounts to B, "PROBABLE," on the MIL-STD-882D scale.

**BOTTOM LINE**

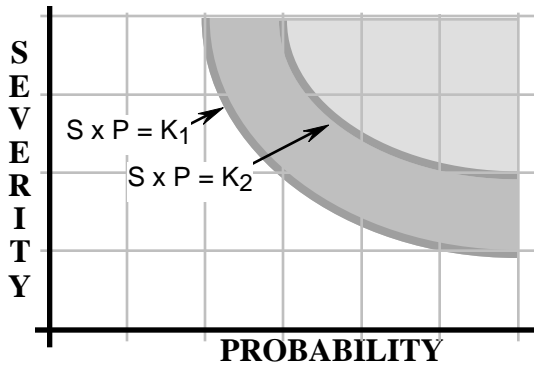
When an estimate must be used, be sure to make known who did the estimating and what method was used. It's bad enough for an estimate to be questionable, but...  
*let there never be doubt where an estimate comes from and how it is arrived at!*

# The Risk Matrix has TWO functions...

***KEEP THEM SEPARATE!***

Risk *Assessment* is NOT Risk *Acceptance*! — Preserve the basics!

- **THAT RISK ASSESSMENT MATRIX** (see generic example, Scrapbook Sheet 00-1) is the foundation tool for evaluating risk using the hazard inventory methods, and a few others.



Its basis is the isorisk contour (see Scrapbook Sheet 84-5), a curve along which risk — taken as the product of the severity and probability of harm — has a constant value. Isorisk contours drawn in the risk plane are smooth, infinitely resolved curves. Two are shown here, for values of risk equal to  $K_1$  and  $K_2$ .

Because quantitative data and analytical resources for numerical risk assessments are often lacking, risk must often be assessed subjectively (i.e., non-numerically). To support this, a matrix can overlaid onto the risk plane.

The isorisk contours can then identify cells within the matrix that form zones exceeding selected levels of constant risk. Subjectively expressed probability and severity scales are assigned to matrix axes as in Scrapbook Sheet 00-1. Thus, the risk plane becomes zoned into judgmentally tractable cells to produce a coarsely resolved matrix as a substitute for the infinitely resolved contours. Resolution is sacrificed, but subjectivity is enabled.

	F	E	D	C	B	A
S I						
V II						
R III						
T IV						
Y						

**PROBABILITY**

- **RISK TOLERANCE PREFERENCES** are expressed by varying matrix zoning. *Zoning need not follow isorisk contours*, and often doesn't.

	F	E	D	C	B	A
S I						
V II						
R III						
T IV						
Y						

**PROBABILITY**

Risk acceptance limits are dictated by the system proprietor or by regulatory edicts, not by the system safety practitioner. A common preference in risk management favors increased aversion to risk as the severity component of risk increases. This is accomplished in the example at left by zoning cells I-E and II-D to lie *below* the isorisk contour originally drawn, to indicate an enlarged area of forbidden risk.

- **ASSESSMENT** and **ACCEPTANCE** of risk are *distinctly separate operations!*

**BOTTOM LINE**

The ruler gages the *length* of the fish you've caught, in calibrated standard units of measure. But, it's the Game and Fish Commission that decides what length you can keep! These two functions are *separate*. *Keep them that way!*

## — Beware of Fault Tree

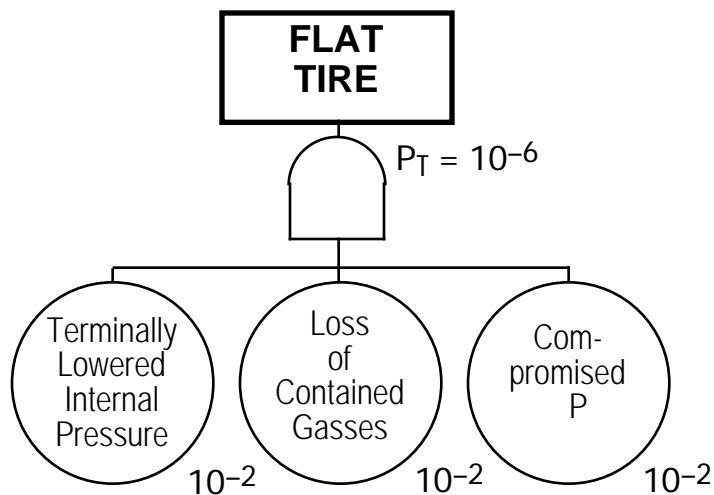
### DOUBLE-TALK!

...a *little* of it'll falsify a *lot* of  $P_{TOP}$  —

...clever headlines can disguise feeble systems!

- **FAULT TREE FLIM-FLAMMERRY IS UBIQUITOUS!** (For opportunities, see Scrapbook Sheets 86-13, 86-14, and 97-8.) — In constructing a fault tree the snake oil analyst sometimes finds that a probability, either within the tree or at the TOP event, is much too high, and there's neither time nor funding to remedy it. Fraudulent editorializing becomes a substitute for shrewd engineering. The quack analyst has only to re-write, beneath an AND gate and repeated several times, the fault expression found at that vulnerable point within the system. *Voila!* Probability for the vulnerable fault drops magically by several — or by *many* — orders of magnitude!
- **HERE'S AN EXAMPLE** that'll demonstrate the point — Notice that the event **FLAT TIRE** has simply been rewritten several times, each expressing that same TOP event, represented using terminology that differs slightly from the others and from TOP event itself.

The effect has been to falsely lower  $P_T$ . Unwary reviewers won't notice this mischievous subtlety, particularly if it has been embedded down in the obscure lower reaches of the tree.



- **BE ALERT** to the possibility that your own fault tree grower may have done something like this, either out of malice or mischance. And don't let the tree that *you* are developing do this. It can happen even to *veteran* fault tree arborists! You've got to check more than the arithmetic — fault trees are all about *LOGIC!*

#### BOTTOM LINE

You can call a catastrophe a calamity, and a cataclysm, and a tragedy, and a mishap, and an accident, and... But once you give it a name in a fault tree, *stay with it*, or you're at risk, and in danger, and under threat, and in peril, of demolishing your logic!

## Assessing Risk?

Be wary of *LUMPING* targets...

***KEEP THEM SEPARATE!***

Sometimes, even the *Standards* encourage chicanery — Stay honest!

- **WHEN ASSESSING RISK** and arriving at a subjective evaluation of its severity component, we're often guided by the stepwise scales found in the various standards that direct our practice. Here are examples for just one of the risk severity levels, as they appear in two, often-used, and reputable standards — other examples are easily be found:

Description	Category	Environmental, Safety, and Health Result Criteria
Critical	II	Could result in permanent partial disability, injuries <b>or</b> occupational illness that may result in hospitalization of at least three personnel, loss exceeding \$200K but less that 1\$M, <b>or</b> reversible environmental damage causing a violation of law or regulation. from MIL-STD-882D

Class II - Critical - A condition that may cause severe injury **or** occupational illness, **or** major property damage to facilities, systems, equipment, or flight hardware.  
from NPG 8715.3

- **THE PROBLEM** — Notice the repeated appearances of that conjunction “**or**” in defining the severity level in the standards. That “*or*” can be the source of badly misdirected risk assessment. First, picture a hazard, having some particular probability of occurrence, that threatens hospitalizing three people, *and* facility destruction exceeding \$200K, *and* illegal but reversible environmental damage, etc. Next, picture a hazard posing a threat to just *one* of those resources, but at the same severity and probability level. Which hazard contributes the greater risk to the system? *BUT* — unless we take special care, these two hazards may be scored as posing equal risks, with the hazard that threatens *multiple* targets appearing to pose no greater risk than the hazard threatening just that *one* of them!
- **THE CURE** — *Separate* the targets! Those individual targets have separate outcomes. Separate outcomes amount to separate hazards. Each source-mechanism-outcome combination counts as a discrete hazard, apart from all other hazards. (See Scrapbook Sheet 98-1.) *Separately* assess risk for each source-mechanism-outcome combination!

### *BOTTOM LINE*

Your insurer charges you a higher premium rate if you protect *both* your home *and* its contents against fire loss than if you insure just *one* of these. That's because *he* recognizes the distinction between **and** and **or**. Be sure that *you* recognize it, too!

## — RELIABILITY ENGINEERING...isn't it *ENOUGH?* Why *Do* SYSTEM SAFETY, anyway? —

...tools of both trades are similar, but their uses have important differences!

- “**RELIABILITY ENGINEERING** ...if you'll just do *it*, then you won't *need* System Safety.” That's an often-heard comment. Is it true? After all, these two disciplines use remarkably similar analytical techniques which are often co-functions of one another. But let's examine the *separate purposes* of these two important practices:

### RELIABILITY ENGINEERING...

explores and evaluates the probability that the system will perform on command, at the time of need, and will to continue to function throughout the period of need with performance undiminished below a desired level, without regard for the penalty of failure to do so.

Almost, but not quite,  
co-function opposites!

### SYSTEM SAFETY...

explores and evaluates the probability that the system will fail to function, at any time, in a way as to result in harm, *and* evaluates the magnitude of the harm to be suffered as a consequence of the failure. (The combined probability and magnitude of harm constitute risk.)

- **THE PRINCIPLE DIFFERENCE?**

Notice that Reliability Engineering concerns itself exclusively with the *probability of success*, whether losses may

occur or not, whereas System Safety concerns itself with *both* the probability of failure *and* its severity penalty.

- **THAT DIFFERENCE** means you *may* actually benefit by using *both* disciplines, in deserving cases. Otherwise, use Reliability Engineering for “Critical Mission” cases, where your concern is that the system “must” succeed, and use System Safety where your concern is for risk as a component of the overall cost of owning and operating the system. Select your discipline(s) with care!

- **EXAMPLES:** (1) A handgun may be extremely *reliable* at firing when the trigger is squeezed. Is it “safe?” That'll depend on the circumstances of the overall “system” in which it's operated: locale (crowded mall or barren desert), user's training, etc. (2) Consider a rocket motor. Features intended to make it more *reliable* at launching on command make a spurious uncommanded firing more likely.

See, also, Scrap-  
book Sheet 95-1.

### BOTTOM LINE

On a drive to the airport, are you concerned with the probability that you'll get there in time?  
...or the probability that you *won't*, and the penalty you'll pay to re-ticket on a later flight?

# It has *never* failed — not yet! *So... now* what's the probability it'll fail when next operated?

You don't *have* to have multiple *failures* to get a trustworthy *MTBF!*

“We’ve made 250 consecutive runs (or operations, or trials, or what have you) *without a failure!* In fact, this system has *never* failed! So, what’s the probability of a failure for the *next* run — or next operation, or trial)?” That’s a very practical question. It’s often asked.

If we’ll settle for a 95% confidence level — i.e., a 5% probability of error, and if we can make certain assumptions (see box), the “**Rule of Three**”<sup>\*</sup> gives an approximate upper limit,  $P_{Fmax}$ , for failure probability:

**ASSUMPTIONS:**

- System failure behavior is stochastic (i.e., random, without aging / wear out).
- System service and environmental stresses have been and will remain unchanged.

$$P_{Fmax} \approx \frac{3}{N} \left. \vphantom{\frac{3}{N}} \right\} \text{ where: } N = \text{number of consecutive, failure-free runs, and } P_{Fmax} = \text{maximum failure probability per run.}$$

The  $P_{Fmax}$  value found here is slightly above a “true” value from the Poisson exponential distribution. This pessimistic bias is 16% for  $N = 10$ , drops to 5% for  $N = 30$ , and  $< 0.5\%$  for  $N > 300$ . The plot below is without this bias. (Log-log scales make the difference too small to notice.) The table in Scrapbook Sheet 97-1 is based on this rule-of-three.

<sup>\*</sup>For an uncomplicated derivation, see Hanley and Lippman-Hand, “Interpreting Zero Numerators”, JAMA, Vol. 249, No. 3, 1983.

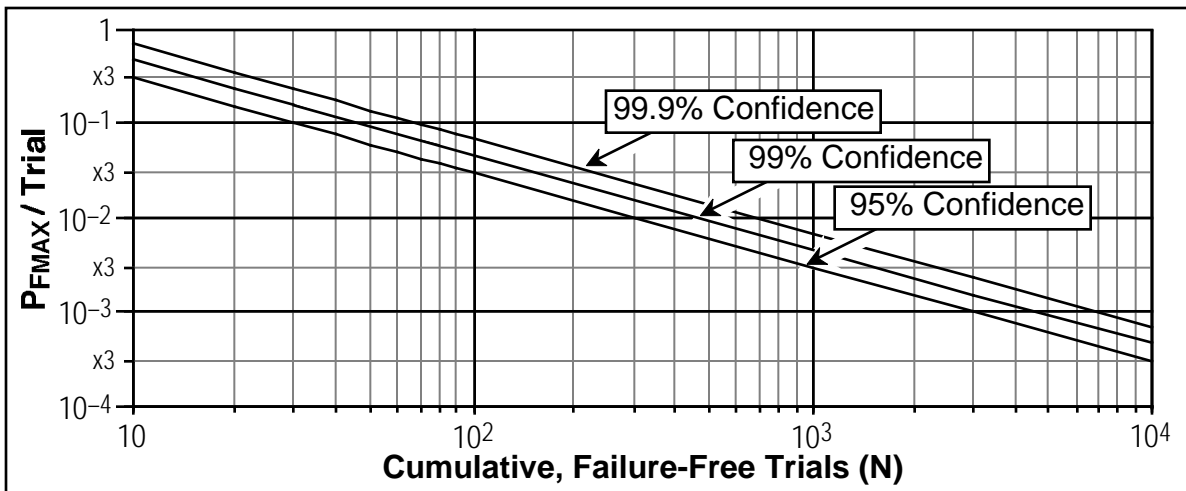
Applying this relationship to our practical case of 250 runs without a failure:  $P_{Fmax} \approx \frac{3}{250} = 1.2 \times 10^{-2}$

Thus we can say, with 95% certainty of being correct, that the probability of failure for the next run does not exceed 1.2 percent.

If greater confidence is needed:  $\left\{ \begin{array}{l} \text{For 99\% confidence: } P_{Fmax} \approx \frac{4.6}{N} \\ \text{For 99.9\% confidence: } P_{Fmax} \approx \frac{6.9}{N} \end{array} \right.$

A least value of Mean Time Between Failures is also easily found:

$$MTBF_{min} \approx \frac{N}{P_{Fmax}} = \frac{1}{1.2 \times 10^{-2}} = 83.3 \text{ runs}$$



**BOTTOM LINE**

If we have to operate a system to destruction many times to determine the probability that operation will destroy the system, we’ll have many destroyed systems on your hands, *and* we’ll have passed the point many times at which we could have declared a failure probability.



— So, you've IMPROVED the SYSTEM!  
 ...*now*, how d'ya *PROVE* you've improved it? —

...*verifying a fix can consume more effort than making it!*

- **Remember your fleet of those old Mk-II Silage Augers?** They had a demonstrated long-term, lifetime track record of 12 failures in every 100,000 hours of use. Thus, their long-term failure rate could be inferred as  $1.2 \times 10^{-4}$  per hour of exposure. But wait — just 2000 operating hours ago, you made an engineering design modification intended to give a substantial reduction in the failure rate. Gratifyingly, there's been *not one failure* since that modification! So, hasn't improvement been demonstrated?

Let's take an unsophisticated look at what we can now say about the change that the modification has made in failure probability. What would have been the probability of failure for the old, *unimproved* system over those 2000 recent operating hours? Using the rare event approximation (from Scrapbook Sheet 97-3) it's...

$$P_F \approx \lambda T = (1.2 \times 10^{-4}) \times (2 \times 10^3) = 0.24$$

That means there was a 76% probability of observing not even one failure during that 2000-hr, post-fix period of observation, and that's with the old, unimproved system. That's not very satisfying verification that the system has been improved!

- **What'll it take to prove improvement?** How many failure-free operating hours are needed to establish, with confidence, that we've improved the system? We can find a break-even point using the "Rule of Three" from Scrapbook Sheet 02-3; the assumptions that were made there apply here, as well:

$$P_{FMAX} \approx \frac{3}{N} \} N \approx \frac{3}{P_{FMAX}} = \frac{3}{1.2 \times 10^{-4}} = 2.5 \times 10^4$$

Thus, not until 25,000 consecutive failure-free hours of operation have accumulated for the newly modified system can we say with 95% certainty that the new failure probability does not exceed the previous one. Even *more* failure-free operating experience must be accumulated to verify that an improvement has been made!

While more sophisticated methods exist to carry out such analyses as these (e.g., applying Bayes theorem), they are worthy of trust only if certain assumptions concerning failure distribution can be made with confidence. Verifying those assumptions also requires large bodies of performance data.

*BOTTOM LINE* —

If it took a lot of operations to prove that failure probability was *low*, it's going to take a lot of operations to prove that it's been *lowered!*

— Is this system *SAFE?* ("No," is a pretty good answer.)  
Is it OK to operate?

WHO makes that decision, and HOW? —

Roles of Risk *MANAGEMENT* and of Risk *ACCEPTANCE* are often confused!

- **DECISIONS AS TO THE ACCEPTABILITY OF RISK** fall in a realm that's not usually accessible to the Safety Professional. Let's look at *why*:
- **TO JUSTIFY UNDERTAKING AN ENTERPRISE** or operating a system, a simple relationship between gain and loss and their probabilities must apply:

$$G \times P_G > S \times P_F \quad \left\{ \begin{array}{ll} G = \text{Potential Gain Amount} & P_G = \text{Probability of Gain} \\ S = \text{Potential Loss Amount} & P_F = \text{Probability of Loss} \end{array} \right.$$

Simply put, the amount to be gained in an undertaking times the probability of the gain must exceed the amount that's at risk times the probability of failure. If this relationship is not satisfied, the enterprise is doomed to eventual failure. It's this relationship that governs all money-making lotteries. It's the principle that underlies all successful gaming.

- **WHO'S IN CHARGE** of the two sides of this expression? The Safety Professional should be proficient in working with that right hand side. Potential Loss is **SEVERITY**, after all, and the Probability of Loss is the **FAILURE PROBABILITY** that, when multiplied by the severity of the harm that might be caused, results in our familiar system safety concept, **RISK!** (Scrapbook Sheet 84-5.) Thus, the right hand side is all about **RISK ASSESSMENT**. The left hand side has to do with the prospect of gain. Except in rare cases, it's much too murky for the Safety Professional. Gain, i.e., profit, is the responsibility of the System Proprietor / Management. The Safety Professional's role is to provide Management all the realistic advice possible about the amount of risk, how it is assessed,\* and how it might be lessened.
- **ARE THERE EXCEPTIONS TO THE RELATIONSHIP?** There *are!* An important one arises when the *amount* at risk is so great that, if it *is* lost, the enterprise cannot recover. Recovery from loss must be possible unless there is a willingness to sacrifice all.
- **FINALLY**, remember that failing to conform to a code, standard, or regulation can lead to a form of loss that can be *quite severe!* Systems must forever be codeworthy, lest the Proprietor / Manager suffer more-than-casual anguish!

\*Scrapbook Sheet 01-8 treats roles of the Risk Assessment Matrix in both risk *assessment* and risk *acceptance*.

**BOTTOM LINE** —

*RISK* is the province of the Safety Professional. He should make himself as skillful as possible at divining its amount and communicating the result to Management! Whether to *accept* risk is more than a management prerogative. It's a management *imperative!*

# — Budgeting countermeasures for max effect? Watch out for *Fault Tree Flimflammetry!* —

*...Too much risk and too few funds? Be careful climbing a fault tree!*

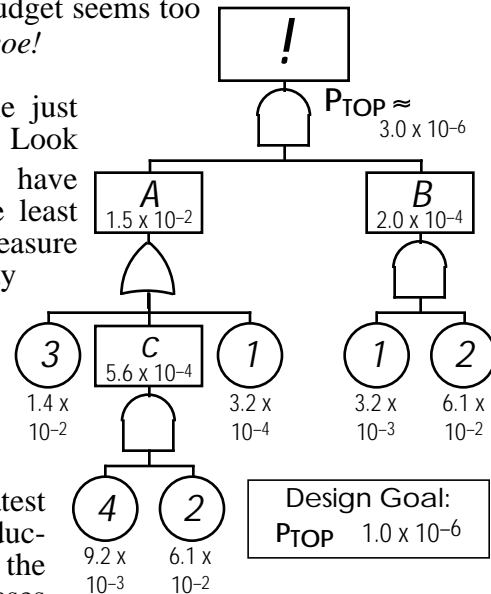
- So... we've grown a fault tree for failure of a critical system function, and we've propagated initiator probabilities upward only to find that TOP probability is a little too high. And the remaining budget seems too enfeebled to support a major design overhaul. *Oh, woe!*

But shouldn't the tree show us where to sprinkle just a few resources to lower  $P_{TOP}$  with greatest effect? Look at those fault tree initiators. Which ones have probabilities that can be lowered the most, at the least cost? Let's price a "best reasonable case" countermeasure for each initiator, and compare their probability reductions:

	$P_F$	$\Delta\$$	New $P_F$	% $\Delta$
1	$3.2 \times 10^{-3}$	48,500	$9.7 \times 10^{-4}$	69.7
2	$6.1 \times 10^{-2}$	123,400	$8.8 \times 10^{-3}$	85.2
3	$1.4 \times 10^{-2}$	6,450	$6.2 \times 10^{-5}$	99.2
4	$9.2 \times 10^{-3}$	12,000	$3.9 \times 10^{-6}$	99.9

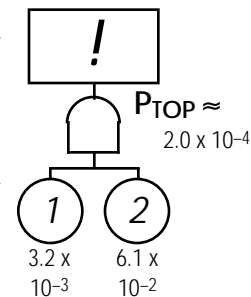
Clearly, the payoff is best for initiators 3 and 4 — i.e., they give the greatest probability reductions (% $\Delta$ ) for the least cost increases

( $\Delta\$$ ). The probability reductions for initiators 1 and 2 are much less, and costs are much greater. Assuming that adopting the new countermeasures for 3 and 4 will adequately reduce  $P_{TOP}$ , no further analysis seems warranted.



- **But**, now look seriously at the logic of that tree. Just what effect do 3 and 4 really have on TOP? Notice that TOP occurs *only* if there are co-existing faults by 1 and 2! Notice, also, that faults by 1 and 2 *alone* are sufficient to *produce* TOP! In other words,  
*3 and 4 play no part in triggering TOP!*

The tree is redrawn here, to tell the truth. That original tree with its  $P_{TOP} \approx 3.0 \times 10^{-6}$  was lying to us! The true  $P_{TOP} \approx 2.0 \times 10^{-4}$  is actually *much worse!* So... it's time to apply for more funding and redesign the system, or accept the risk, or just give up and go home!



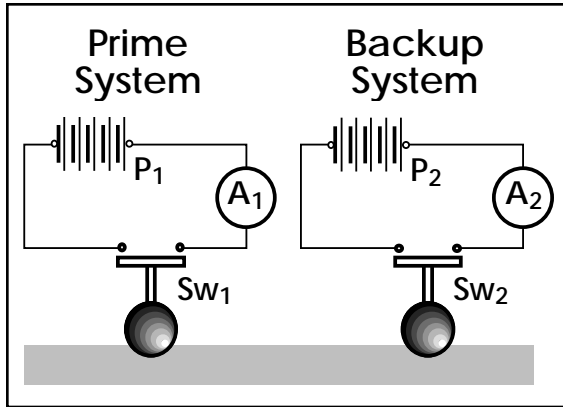
- **None of this would have happened** to us if, before we quantified  $P_{TOP}$ , we'd "pruned" that initial tree to its basic elements — i.e., to its *minimal cut sets*. Minimal cut sets are *least* groups of initiators which, upon occurring, induce TOP. And for this tree, there's only one minimal cut set. It's 1 and 2. Also, in that table above, we should've been finding not the probability reductions of individual countermeasures, but the overall reduction that each one contributes to lowering to  $P_{TOP}$ .

**BOTTOM LINE**

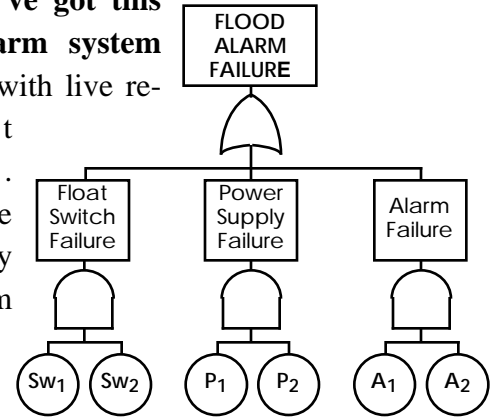
Fault tree skulduggery is easy to perpetrate.  
Chances are, you won't even know when you've done it!  
**WATCH THE LOGIC!**  
Be not bamboozled!

# — Fault Treeing Redundancy? ...then Model the *FUNCTIONS*, not the *PARTS LIST!* —

*Sometimes, you can be wrong by just by trying to be thorough!*



• So, we've got this flood alarm system (at left), with live redundant backup. Both the primary system and the redundant



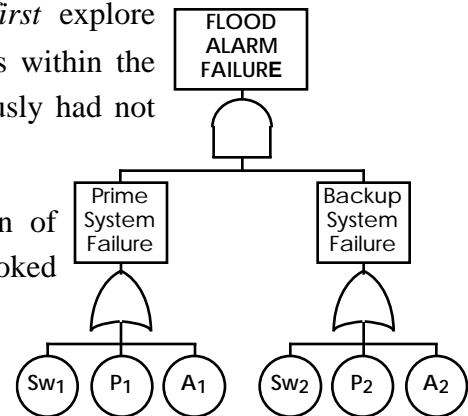
backup have float switches (Sw), power supplies (P), and alarm features (A). We've developed a fault tree (at right) to explore Flood Alarm Failure. (Our analysis presumes the system has been challenged by a flood.) Our tree has a lovely symmetrical charm about it! And it displays failures of each of the components — no omissions. Those three AND gates represent our reassuring redundancy against system failure. Good design!

• **But**, look at the *system*, not at the *tree*. Ask what happens if there are co-existing faults of, let's say, P<sub>1</sub> and A<sub>2</sub>, or by Sw<sub>1</sub> and P<sub>2</sub>, or by A<sub>1</sub> and Sw<sub>2</sub>? The system is *defunct!* But these and many other combinations of faults DO NOT PRODUCE PATHS TO THE TREE TOP! Our fault tree is faulty!

• **Let's re-develop the tree**, as at right. Here, we *first* explore faults of subsystem functions, *then* functions of items within the subsystems. Those combinations of faults that previously had not produced the TOP event clearly do so now.

• **Why?** Fault tree analysis is a top-down, exploration of *functional paths to the top event!* Our first tree had looked at *parts*, not at *functions!*

• **What else?** We've neglected common-cause threats. (See Scrapbook Sheets 86-4 and 87-4.) Do not redundify using identical components!



**BOTTOM LINE**

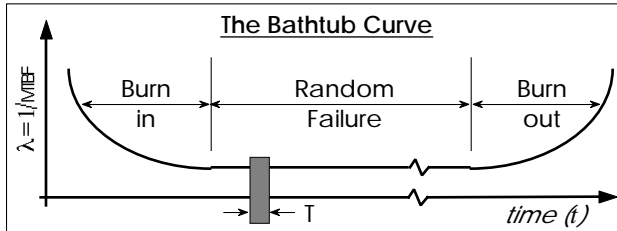
A fault tree is a representation of system fault logic, *not* a display of agglomerated, like parts! Start the analysis at the top of the tree *and* at the top level of system function, *at the same time!* Then work systematically downward, through both.

## — Parts Replacement to reduce $P_F$ ...

*Does it do the job? —*

*If it's not wearing out, should we swap it out before it goes bust?*

- A critical item in our system has an **MTBF** of 800 hours. It's been that way for years. It



has a demonstrated record of staying on the flat Random Failure bottom of its own bathtub curve for *many* **MTBFs**. (See Scrapbook Sheet 95-2.) This critical item is in a system that has a desired duty cycle of 400 hrs. That gives us a failure

probability for this item, during that duty cycle, of:

$$P_{F(400)} = 1 - e^{-T} = 1 - 2.718^{-\frac{400}{800}} = 0.3935 \text{ (from Scrapbook Sheet 95-3)}$$

A failure probability of nearly 40% is *high!* That's why we've been so annoyed about the unscheduled down time we have during nearly half of those 400-hr duty cycles! Why don't we reduce  $P_F$  by replacing that offending item frequently, let's say every 200 hours, at an available pause point midway of that 400-hr duty cycle? That'll put a fresh player in the game more often than we have now. (All of our parts are past Burn In and well into Random Failure.) What'll be the effect of this "parts refreshment" plan on failure probability? For the 200-hr period that'll be assigned to each of the two items that we'll now use in the duty cycle...

$$P_{F(200)} = 1 - e^{-T} = 1 - 2.718^{-\frac{200}{800}} = 0.2212$$

That's a *big* reduction in  $P_F$ , *but* we've now got *two* of these things in back-to-back 200-hr exposure intervals. If either one fails (1 OR 2), we're in the soup. Let's **IP** through that OR to see how hot the soup is (Scrapbook Sheet 87-6):

$$P_{F(200 + 200)} = 1 - [(1 - 0.2212) (1 - 0.2212)] = 1 - (0.7788)^2 = 0.3935$$

Now, that is a very familiar number! *It's the same  $\approx$  40% we started out with!*

- **Why is this?** It's because we're in the Random Failure period for *both* parts, where (hence **MTBF**) is constant. *The system can't tell the replacement part from the original!*

Another way of saying this:

**PREVENTIVE MAINTENANCE BY SIMPLE REPLACEMENT OF PARTS THAT FAIL AT CONSTANT RATES DOES NOTHING TO REDUCE FAILURE PROBABILITY!**

**BOTTOM LINE**

Putting a new pitcher in the game may win it for you,  
*but not of his performance is the same as the one you just pulled out!*  
 Don't discard good operating hours unless you're sure of a gain! When you practice preventive maintenance, be certain you know what it is you want to prevent!

## — Using the good old Poisson Distribution?...

*Then be prepared for dispute —*

Deciding whether risk is acceptable? OR Designing a spare parts inventory?  
Those different *needs* need different *methods*!

- **That simple exponential distribution model** for failure probability (e.g., Scrapbook Sheets 95-3, 97-3, et al). It has many detractors who argue that it's inaccurate. It's

$$P_F = 1 - e^{-T}$$

T = Exposure Interval  
= 1/MTBF  
= Napierian base (2.718...)

?

certainly unsophisticated. (That means it's not complicated, and it's easy to apply!) And it often is inaccurate! Its fundamental assumption that failure rate ( ) is constant over the useful lifetime of the system is sometimes flawed. (Remember, it does *not* apply to the

wear-out end of the bathtub curve!) Unfortunately, it takes a lot of failures to prove that varies enough to justify using a more elaborate model. And with new designs, high-tech systems, developmental systems, and cutting-edge technology, when something fails, we make a change to improve the system and reduce  $P_F$ . We then have a "different" system. The previous failure data no longer apply. So... we begin collecting data all over again.

- **QUESTIONS TO ASK:**

**Do you need System Safety** for a new design, or new configuration, or new application?  
*Use the simple exponential model until you've got a meaningful body of failure data.*

**Are you doing a Reliability Analysis** on a mature system with a lot of performance data available from field use? *An elaborate model is very likely justified.* (See below.)

- **When *IS* a sophisticated model warranted?** You're justified in moving to a more elaborate model when: (1) you are certain nothing influencing  $P_F$  has changed or is going to change — e.g., design, stresses, maintenance, method of operation, etc. **AND**; (2) you have a body of data that will support it. How many failures do you need, to model failure meaningfully? **RULE OF THUMB:** If you've had at least 15 failures, and the last three have affected  $P_F$  for the current model by more than 14%, you may have enough failure data to warrant a fancier model. (Let today's model "settle out" before shifting to tomorrow's.)

— ***BUT...*** What is it you've *analyzed*, anyway? —

**Most of the mistakes** made in system safety analyses come not from the analytical technique used but from errors in constructing the conceptual model that gets analyzed.

REMEMBER...

**YOU NEVER ANALYZE A SYSTEM!**

**YOU ONLY ANALYZE A CONCEPTUAL MODEL OF A SYSTEM!**

**BOTTOM LINE**

Move to the micrometer only after you have confidence  
the tape measure won't give you the answers you need.

## — Why use a *LONG MTBF...* for a *SHORT-HAUL SYSTEM?*—

*MTBF has more than one way to hornswoggle the analyst!*

- **The Specs call for a Mean Time Between Failures of 114 years** for a full-up, round-the-clock system. But this thing's only going to be operated for six months. That gives it a duty cycle shorter than 0.5% of a whole **MTBF**! Doesn't this seem unnecessarily risk averse? After all, considering the rate at which technology advances, this thing'll be obsolete in less than a fourth of an **MTBF**.
- **But, wait... it's an especially Critical Function** this system is going to perform. We must have confidence that the probability of failure to perform that function is no worse than  $10^{-6}$  per hour over those six months — *not* an uncommon requirement!
- **What's MTBF for an Hourly Failure Probability of  $10^{-6}$ ?** To find, out we can use the exponential distribution function (Scrapbook Sheet 95-3):

$$P_F = 1 - e^{-T} \quad \left\{ \begin{array}{l} \text{where: } T = \text{exposure interval} \\ = 1/\text{MTBF} \\ = \text{Napierian base (2.718...)} \end{array} \right.$$

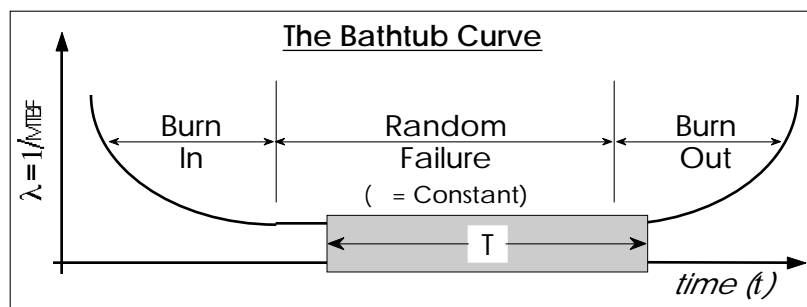
Let's substitute for  $P_F$ , rearrange, and solve this thing for **MTBF**:

$$\text{MTBF} = \frac{T}{\ln\left(\frac{1}{1 - P_F}\right)} \quad \left\{ \begin{array}{l} T = 1 \text{ hr} \\ P_F = 10^{-6} \end{array} \right. \quad 10^6 \text{ hr} \quad 114 \text{ yrs}$$

*This is that same 114 years we started out with!* Notice that we'd have got the same result using the rare event approximation (Scrapbook Sheet 97-3):

$$P_F \approx T \cdot \lambda \rightarrow \text{MTBF} = \frac{T}{P_F} = 10^6 \text{ hr}$$

- **If T is LARGE**, then we may have yet *another* problem! We're possibly beyond the random-failure, flat-bottom of the bathtub curve and into Burn Out, where  $\lambda$  rises. *Don't let that happen!*



Finally, remember that **MTBF** is not life expectancy! (See Scrapbook Sheet 95-3.)

**BOTTOM LINE**

Don't confuse distance with rate.  
We don't have to drive 100 miles  
to appreciate the peril of driving 100 miles an hour!

## — “Spreading” to reduce RISK?...

Don't forget to look at the *cumulative* effect! —

*Can we lower Risk by breaking it into small pieces? NOT SO OFTEN!*

- We've got 3000 pounds of Explosive Class/Div. 1.1 VDP™ Roach Repellant, formerly stored in a bunker for later processing at a plant site. We were spooked at the prospect of losing our goop in a lightning-induced ignition event. So... we've “spread” the risk by breaking it into three, 1000-pound lots that'll be stored in three, separate, widely-spaced bunkers. Clearly, we've divvied up the severity component of something or other. *BUT*, let's look at the Before and After RISK ARITHMETIC, first *in toto* and then by parts:

Original Total Risk for the lightning-strike hazard is the simple product of the Probability of ignition and the Severity of the explosion event:

$$R_{T(\text{Before})} = P_T \times S_T$$

With the three-way “partitioning” of the stuff into bunkers A, B, and C, Total Risk is now:

$$R_{T(\text{After})} = P_A S_A + P_B S_B + P_C S_C$$

But, because we've broken the quantity into three, separate, equal volumes, notice that the severity for each of them is now one third of the original severity:

$$S_A + S_B + S_C = \frac{S_T}{3}$$

...and, each of the three distantly separated bunkers now faces the same lightning hazard as did the original one, so...

$$P_A = P_B = P_C = P_T$$

So... Total Risk now looks like:

$$R_{T(\text{After})} = 3 \left( P_T \frac{S_T}{3} \right) = P_T \times S_T = R_{T(\text{Before})}$$

...which is *exactly* what we started out with!

- **So, what good have we done, if any?** We've reduced the maximum loss of VDP™ we're likely to suffer in a single event. Beyond that, *we've done nothing at all to reduce total risk!* If, however, loss of the original 3000 pounds would wipe out our entire enterprise but losing 1000 pounds would not, we've made an interesting change: We've increased the probability of losing 1000 pounds by a factor of three, but we've very substantially reduced the probability of a 3000-pound total wipeout — assuming we haven't got a common cause available to light off all three at once! (See Scrapbook Sheet 86-4.)

*BOTTOM LINE*

*“When we're on the march, we march single-file, far enough apart so one shot can't go through two men.”*

*Standing Orders — Rogers' Rangers, 1759*



— Are some systems *“Accident Prone?”*...  
 Don't *condemn* without *calculating!*—

*An apparent “cluster” of hits may not mean what most folks think!*

- **A FLEET OF 82 IDENTICAL SYSTEMS** (or components, or what have you) operating in identical 8-hr, 5-day service has racked up a ten-year failure history of 69 crashes.

$$P_{(n)} = \frac{(m)^n \cdot e^{-m}}{n!}$$

$P_{(n)}$  = probability, per system,  
 of  $n$  crashes  
 $n$  = crash count  
 $e$  = Napierian base (2.718...)  
 $m$  = long-term average  
 crash count per system  
 ( $\frac{69 \text{ crashes}}{82 \text{ systems}} = 0.841$ )

Thirty-three of the 82 systems have had no failures. However, four look suspiciously “sick,” one with four crashes and three with three crashes each. *Should we replace those four big offenders?* Let’s use the Poisson exponential distribution to help us decide. We used its first term in Scrapbook Sheets 95-3, 97-3, 01-7, 02-8, et al to find the probability of one or more failures. Here, instead, we’ll use the full expression to compute the

CRASH COUNT	NUMBER OF SYSTEMS SUFFERING CRASHES	
	Actual	Predicted
0	33	35.4
1	34	29.7
2	11	12.5
3	3	3.51
4	1	0.737

expected numbers of failures based on the presumption of pure randomness. Then we’ll compare the actual outcome with our “predictions”:

- **SO, WHAT DO WE DO NOW?** Our fleet has behaved about the way simple randomness predicts, based on this 10-year, 0.841 crash rate. If we replace those four big offenders and make no other changes, we can expect *the same results* over the *next* ten years! But it’ll probably be some *other* system in the fleet that has the four crashes. We have *much* more reason for concern about lowering the rate for each member of the overall fleet of 82 than we have for worry about any single system!
- **OCCUPATIONAL COROLLARY...** Now, picture this same problem but substitute workers for systems and substitute workplace injuries for crashes. How would we feel about a worker who had four injuries during a period when 33 others, doing the same job, had *none*? Is he “accident prone?” Should we retrain him? Reprimand him? Transfer him? But given the nature of randomness, it might be counted as unusual if there *weren’t* a victim of four injuries in that group of 82. *So...* is that four-injury worker a victim of *carelessness* or of *randomness*? ...and shouldn’t we try to get the overall injury rate down before we blame an individual whose roulette wheel has mistreated him?

**BOTTOM LINE**

“Clustering” happens. Don’t be fooled by it! Verify the likelihood of seeing the results for the population probabilistically before you blame any of its members individually.

*Things may be behaving just about as they should!*

# SYSTEM SAFETY SCRAPBOOK

## — Index —

<u>Topic</u>	<u>Sheet No.</u>
Abuses of Systems, excluding from analyses.....	01-4
Accident pron-ness, testing for.....	02-12
Analytical Technique(s)	
Selecting.....	87-1
Top-Down vs Bottom-Up (selecting).....	97-9
Analytical “Types” vs “Techniques”.....	99-1
Assessment Matrix (Risk)	
“Calibrating”.....	00-2
Example matrix.....	00-1
Bathtub Curve	
Modeling failure probability.....	95-2
Relationships to MTBF and failure probability.....	95-3 & 97-3
Bounding — See Scoping	
Checklist of Hazards.....	86-1
Chicanery for lowering risk.....	00-4
Clustering of loss events, diagnosing.....	02-12
Common Causes, Finding and Curing.....	86-4 & 87-4
Cost aspects of System Safety.....	00-6
Countermeasures	
Budgeting for greatest effect.....	02-6
Effectiveness hierarchy.....	83-4
Leapfrog bounding of probability limits.....	96-4
Procedures and human operators as.....	86-6
Selection criteria.....	83-7
Vulnerability reduction methods.....	97-6
Distribution, Poisson, prepare for debate when using.....	02-9
Disclaimers, the need for and an example.....	01-6
Economic aspects of System Safety.....	00-6
Estimating Failure Probability	
Using MTBF.....	01-7
Using upper and lower bounds.....	97-5
Exposure Interval	
For human targets.....	99-2
Importance of, and effect on risk.....	84-4
Failure Modes and Effects Analysis	
Bottom-Up analysis (compared to Top-Down).....	97-9
Brief description — advantages and shortcomings.....	87-1
Critical circuit considerations.....	83-2
Hazard Inventory Technique weakness.....	97-10

Review hints.....	84-1
Scoping.....	96-1
When to revisit / revise.....	97-7
Failure Probability (See Probability)	
Fault / Failure Nomenclature.....	86-11
Fault Tolerance.....	00-7
Fault Tree Analysis	
Brief description — advantages and shortcomings.....	87-1
Challenges, omitted and correcting for.....	86-14
Common causes, finding and curing.....	86-4 & 87-4
Diagnostic tricks.....	86-7
Flimflammy.....	02-6
“Flip-TOP” test to verify gate logic.....	86-13
Functions, to be modeled rather than parts.....	02-7
Ipping for OR-gate exact solutions.....	87-6
Overgrowth avoidance — how far down to analyze?.....	86-5
Probability accuracy (TOP), when needed.....	00-3
Probabilities, failure data for TOP comparisons.....	87-3
Rare-event approximation for OR-gated events.....	87-5
Revisiting / revising — when to do it.....	97-7
Review hints.....	83-6
Scoping to avoid fault kudzu.....	86-10 & 96-1
Selecting / naming faults, and other guidance on construction.....	86-8
State-of-component method.....	86-12
Top-Down analysis (compared to Bottom-Up).....	97-9
TOP incredibly low? What’s it mean?.....	97-8
TOP Event Double-Talk to lower probability.....	01-9
When to revisit / revise.....	97-7
Hazards	
Checklist.....	86-1
Definition.....	98-2
Describing.....	98-1
How to find.....	87-2
Naming to reduce confusion.....	84-3
Human Operator Failure Probabilities.....	86-6
Ipping.....	87-6
Iso-Risk Contour.....	84-5
Improvement, proving it.....	02-4
Limitation Statements, the need for and an example.....	01-6
Lumping targets, be wary of.....	02-1
Matrix	
“Calibrating” the Risk Assessment Matrix.....	00-2

Risk Assessment.....	00-1
Two separate functions of.....	01-8
Mission Phasing, Importance of.....	86-3
MORT Logic Flaw.....	86-2
MTBF	
And relationship to failure probability.....	97-3
And the bathtub curve.....	95-2
Don't confuse with life expectancy.....	95-3
Why specify long MTBF for short-term application?.....	02-10
Operational Phasing, Importance of.....	86-3
Parts, replacing to reduce $P_F$ .....	02-8
Poisson Distribution	
Used to analyze "clustering".....	02-12
Prepare for debate when using.....	02-9
Population of hazards, of targets, effect on Risk.....	01-2
Preliminary Hazard Analysis	
Bi-directional analysis (compared to Bottom-Up and Top-Down).....	97-9
Brief description — advantages and shortcomings.....	87-1
Finding Hazards.....	87-2
Hazard Inventory Technique weakness.....	97-10
Review hints.....	96-2
Scoping.....	96-1
Some shortcomings.....	84-6
When to revisit / revise.....	97-7
"Worst-Credible" assessments may be misleading.....	97-11
Probability	
Defending data against challenges.....	97-2
Estimating using bounds and means.....	97-5
Estimating based on MTBF.....	01-7
Failure data for TOP comparisons.....	87-3
Failure probability relationship to MTBF.....	97-3
Fallacious overspecifying.....	97-1
Leapfrog bounding in setting tolerance limits.....	96-4
Numerical failure data for "Bootstrapping" comparisons.....	87-3
TOP probability incredibly low? What's it mean?.....	97-8
Transforming reliabilities to failure probabilities.....	95-1
Unaffected by parts replacement.....	02-8
Programmatic Risk.....	01-1
Quackery for lowering risk.....	00-4
Reliability Engineering, isn't it enough?.....	02-2
Redundancy	
At what indenture level to adopt?.....	83-5

Redundant readouts, disagreeing — which to believe?.....	83-3
Reports on Analyses, precautions to take.....	01-5
Review Hints	
Fault Tree Analyses.....	83-6
Failure Modes and Effects Analyses.....	84-1
Preliminary Hazard Analyses.....	96-2
Revising Analyses, when to do it.....	97-7
Risk	
Apparently equal risks may not really <i>be</i> “equal”.....	97-4
Assessment Matrix, see Matrix	
“Calibrating” the Assessment Matrix.....	00-2
Exposure Interval, effect of.....	84-4
Evaluating look-alike systems.....	86-15
Iso-risk contour.....	84-5
Lowering, through Chicanery / Quackery.....	00-4
Options for managing excess.....	86-9
Population of Targets/Hazards, effects on Risk.....	01-2
Programmatic.....	01-1
Risk Plane.....	84-5 & 97-11
Risk Stream.....	84-2
Spreading to reduce it — does it work?.....	02-11
“Worst-Credible” assessments may be misleading.....	97-11
Rule of Three.....	02-3
Safety, has it been achieved?.....	02-5
Scoping Analyses — Bounding to Describe and Confine Effort	
General.....	96-1
Fault Trees.....	86-10
PHAs and FMEAs.....	01-3
Expectations of System Owner Care.....	01-4
Single Point Failures vs Failure Probability.....	83-1 & 86-15
Spreading to reduce risk — does it work?.....	02-11
System Safety, when to use?.....	00-5
Targets, be wary of lumping.....	02-1
Thorough Analyst’s Penalty.....	96-3
“Types” of analysis, vs “Techniques”.....	99-1
Vulnerability reduction methods.....	97-6
When to analyze.....	00-5
“Worst-Credible” assessments may be misleading.....	97-11
Zero failures, what’s P <sub>F</sub> ?.....	02-3